



University of Nairobi.

MSC: Distributed Computing Technology

CDT 599: Research Project

TOPIC: SECURE CLOUD MIGRATION SERVICE

**TITLE: DEVELOPMENT AND AUTOMATION OF SMEs' MODEL FOR
INFRASTRUCTURE SERVICE-MIGRATION TO CLOUD.**

BY

KINARO. W. ORESTE

P53/85713/2016

SUPERVISED BY

CHRISTOPHER CHEPKEN (PHD)

Declaration

This research project report is my original work and has not been submitted previously for the award of any certificate in any other University or institution.

Signature..... Date.....

Kinaro W. Oreste

P53/85713/2016.

This project has been presented for examination with my approval as the student supervisor.

Signed..... Date

Christopher K. Chepken (PHD).

University Of Nairobi.

Acknowledgement

I would like to express my sincere gratitude to the Almighty God and to all those who gave me their most needed support to complete this study. In particular, I express my gratitude to my esteemed supervisor Dr. Christopher K. Chepken, University of Nairobi for his guidance, constructive criticism and for playing the role of seeing my successful completion of this course. My immense gratitude to all members of my family and more so to Mr. Kinaro Kinyua(dad) for his support and encouragement through the rigorous process of this research journey. I do appreciate the assistance and care of my friends for their motivation during this research work. I am thankful to Mr. Michael Kagiri for his excellent advice during my research work. Finally, I would like to express my gratitude to many others not mentioned, who contributed to this project in one way or another.

Dedication

To Dad who was the best motivator and advisor during this undertaking.

Abstract

In this paper, we present the Infrastructure-as-a-service(IaaS) migration as a process that requires the collaboration of various technical skillsets in an organization. We present the IaaS migration as a process comprising of stages and subtasks that need specialized skills in Cloud Infrastructure Administration, Cybersecurity, Systems development, Network Administration and Business Development. We present deployment of applications to the IaaS cloud as a process consisting of 8 critical stages of 1) Gaining access to the IaaS cloud; 2) Installation of Operating system 3) Installation of App Server;4) Patching Operating system and App Server; 5) Uploading system files to the cloud; 6) Implementing cloud security policies; 7) Configuring DNS management and 8) Testing of system components functionalities. We proceeded to identify the roles of each of the skillsets and how they collaborated during the IaaS migration.

This study then designed and developed an automation tool that supports the collaboration of the identified technical skillsets in organizations during an infrastructure-as-a-service(IaaS) migration. The developed automation tool in this paper enabled Systems developers, Cloud infrastructure administrators, Cybersecurity professionals, Network administrators and Business developers to collaborate in executing the various stages during services migration to the IaaS cloud. The automation tool in this study simplified the complexities of the IaaS cloud migration by providing needed information and fostering skills collaboration during an IaaS migration.

Contents	
Declaration	2
Acknowledgement	3
Dedication	4
Abstract	5
List of figures	8
List of Tables	9
List of Acronyms and Abbreviations	10
CHAPTER ONE	11
1.1. Background of Research	11
1.2. Problem Statement	12
1.3. Research Objectives	13
1.4. Research Questions	14
1.5. Research Significance	14
1.6. Definition of Most Significant Terms	15
CHAPTER TWO	16
LITERATURE REVIEW	16
2.1. Introduction	16
2.2. Cloud Computing in Enterprises	16
2.3. Security in Cloud Migration	18
2.4. Migration to the cloud -Case Kenya	20
2.5. SOA in Cloud Migration	21
2.6. Existing IaaS Cloud Migration models	22
2.7. Cloud Automation Tools	24
2.8. Conceptual Framework	27
CHAPTER THREE	29
METHODOLOGY	29
3.1. Introduction	29
3.2. Research Design	29
3.3. Population Sampling	31
3.4. Data Collection	31

CHAPTER FOUR	34
SYSTEM ANALYSIS AND DESIGN	34
4.1. System Specification	34
4.2 System Analysis	35
4.3 System Design	35
4.4 System Development	40
4.5 System Testing	51
4.6 System implementation	57
CHAPTER FIVE	61
RESULTS	61
5.1. Primary Data Findings	61
5.2. Secondary Data Findings	73
5.3. Discussion	75
5.4. Chapter Summary	79
CHAPTER SIX	80
CONCLUSION	80
6.1. Introduction	80
6.2. Research Objectives Achievement	80
6.3. Limitations of The Study	84
6.4. Future Research	84
REFERENCES	86
APPENDICES	91
Appendix 1: introduction letter to respondents	91
Appendix 2: Research Schedule and Timeline	92
Appendix 3: Budget of Research	93
Appendix 4: Technical Feasibility	94
Appendix 5: Questionnaires or Interview scripts	95
Appendix 6: White box Testing Checklist	99
Appendix 7: Sample Raw Results	100
Appendix 8: Some of the source Code Used	102

List of figures

Figure 1: IaaS Automation Tool Use Case.....	33
Figure 2: IaaS Automation Tool Architecture.....	36
Figure 3: Registration of New Migration project.....	38
Figure 4: Roles and Permissions Assignment	38
Figure 5: Migration stages and tasks definition.....	39
Figure 6: Registration of Team Members.....	40
Figure 7: Migration Stages Execution.....	41
Figure 8: IaaS automation tool Login Page.....	42
Figure 9: Registration of a new project.....	42
Figure 10: Registration of a New Migration Stage.....	43
Figure 11: Tasks in Migration Stages Registration.....	43
Figure 12: Migration roles Registration	45
Figure 13: IaaS migration project team member Registration	45
Figure 14: New User Account Setup notification.....	45
Figure 15: Classification of User roles and tasks	45
Figure 16: Migration stages Execution.....	48
Figure 17: Black Box testing results.....	49
Figure 18: Automation tool Functionalities testing findings.....	52
Figure 19: White box Testing Findings.....	54
Figure 20: Technical Skills distribution in IaaS migration.....	65
Figure 21: IaaS security types during IaaS migration.....	68

List of Tables

Table 1: Client workstation Features used in system development.....	55
Table 2: Development server workstation features.....	56
Table 3: Hosted on Cloud Server Features.....	56
Table 4: Automation tool Development Environment Features.....	57
Table 5: IaaS Migration Experience.....	58
Table 6: IaaS Migration central tendencies.....	61
Table 7: IaaS provider choices	61
Table 8: IaaS Provider responses variance analysis.....	63
Table 9: IaaS Virtual Machines Instances Used.....	64
Table 10: IaaS Virtual Machines responses variance analysis.....	64
Table 11: Technical skills in IaaS actual migration.....	65
Table 12: Tasks and Steps in IaaS migration.....	67
Table 13: Stages in IaaS migration.....	67
Table 14: Security in IaaS migration.....	68

List of Acronyms and Abbreviations

AWS	Amazon Web Services.
IaaS	Infrastructure-as-a-Service.
IAM	Identity access management.
ICT	Information communication Technology.
IT	Information Technology.
IVR	Interactive Voice Response.
LAN	Local Area Network.
PaaS	Platform-as-a-Service.
RBAC	Role Based Access control.
SaaS	Software-as-a-Service.
SME	Small Scale and Medium Scale Enterprises.
SOA	Service Oriented Architecture.
SSL	Secure socket Layer.
VMs	Virtual Machines.
VPN	Virtual Private Network.
VPS	Virtual Private Servers.
WAN	Wide Area Network.

CHAPTER ONE

INTRODUCTION

1.1. Background of Research

Cloud computing is among the most significant technology big trends which have seen most businesses take it up and is of high relevance when used by Small and Medium Scale Enterprises(SMEs) (Candel Haug, Kretschmer and Strobel, 2016). Cloud computing solutions give users different capabilities to store and process their data in third-parties' privately owned data centers (Jamshidi, Ahmad, and Pahl , 2013). In Cloud computing, computing resources such as servers, network, storage, and software are offered at an abstraction over the Internet for remote access. Access to cloud computing services is billed on a pay-per-use arrangement. Cloud services are offered as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) with are deployed in models of Private cloud, Public cloud, community cloud and hybrid cloud. In the context of cloud computing, IaaS enable adopters to deploy own computing resources on provider's hardware for use as services on demand. PaaS allows users access to all facilities that are required in the construction and deployment of web applications provisioned over the Internet. Software as a Service (SaaS), offers its consumers a wide variety of licensed applications provided by service providers on demand for use as services over the Internet (Nabeel,2015). In a Private cloud deployment, the cloud is managed and operated internally and solely by the Organisation. Private clouds contain multiple consumers within an organisation who do not have access to external world data. A Public cloud is owned by an organisation and available for free or at a fee to the general public (Amir and Gupta,2016). A Community cloud is owned by several companies who agree to share the cloud infrastructure. Hybrid Cloud, on the other hand, combines two or more cloud models (Public, private or community).

Cloud services have enabled enterprises to relinquish unnecessary Information Technology(IT) computing resources by pay-and-use only needed resource, which in a way puts a firm in a position of efficient use of its computing resource. In recent times, SMEs are getting wind of these and other important aspects of cloud technology which in return leads them to migrate their systems to the cloud (Astri,2015). Unlike SaaS and PaaS, IaaS poses an attractive model where the consumer has extensive control over network resources, storage, operating systems and their deployed systems. In quenching the consumers' quest for control of their deployments in the cloud, IaaS

offers much-needed flexibility in the manner in which consumers migrate and provision computing resources on the cloud. Whenever an organization is seeking to Rehost its systems to the cloud, Infrastructure-as-a-Service(IaaS) provides the best niche over Platform-as-a-Service(PaaS) and Software-as-a-Service(SaaS). This is because IaaS offers an ability to move a business' IT infrastructure to an outsourced business arrangement with increased control and security of data hosted on the IaaS provider's computing resource(Gupta,2014). IaaS is characterized by Virtual machines whose instances are relayed to consumers on which they configure systems according to their unique requirements. IaaS systems deployment to the cloud is entirely within the responsibilities of the IT department of an Organisation. The IT team needs to have an adequate understanding of IaaS cloud technologies and possess sufficient skills to deploy, adapt and configure systems on Public clouds, Private Clouds or Hybrid Clouds of choice. (Claus, Huanhuan and Ray, 2013).

Automation tools provide different ways of performing tasks in the cloud environment. They ease the cloud processes and administration tasks' complexities of the cloud platform. Cloud automation tools have previously been used to simplify the execution of tasks on the cloud. Their appeal is because they simplify the complexities in executing tasks of cloud administration. Regarding Security, Private cloud deployments are preferred since they provide increased privacy and data security over public clouds. Concerning cost, Private clouds are more expensive to acquire, and for instances where an enterprise is not able to meet the cost requirement of a private cloud, IaaS deployment on a public cloud is considered(Sumit,2014). IaaS cloud security is a serious consideration for both cloud providers and adopters in equal measures. IaaS providers will provide the underlying physical hardware security up-to-the hypervisor. On the other hand, IaaS customers are responsible for security controls relating to their hosted systems (e.g., the Operating system, deployed applications and data) and adaptation of their systems to the IaaS cloud environment. It is also the responsibility of the cloud adopter to implement security measures to ensure secure interactions with their hosted data (Andrikopoulous et al,2013).

1.2. Problem Statement

Cloud computing introduces new career sets and opportunities for IT Professionals. IaaS offers an ability to move a business' IT infrastructure to an outsourced business arrangement with increased control and security of data hosted on IaaS provider's computing resources (Gupta,2014). In a

cloud migration process, having the right composition of expertise skill and implementing the right technologies are major concerns in undertaking the migration project(Claus,2013). Companies that need to move their systems and applications to the cloud will need to hire consultants or have staff with sufficient skills to migrate systems to the cloud. For Small and Medium Scale Enterprises (SMEs), hiring staff or invocation of expert consultants attracts huge costs which may not be realized in most scenarios (Nicholas,2013). The remedy to avert these huge costs for SMEs is to build staff capabilities and skills ahead of a migration process (Yousif,2016). Migrating systems to the IaaS clouds is not an easy task. IaaS Cloud migration tasks introduce complexities during the migration process. Common migration procedures are not defined, and this leads to over-reliance on migration experts' experience in performing the actual migration. The actual cloud migration poses critical risks of exposing sensitive and vital information about a company (Andricopoulus,2013).

The actual process of migrating systems to the IaaS clouds should be right from the initialization to the end. With complexities and challenges experienced during IaaS cloud migration, common migration patterns could be established within a given set of enterprises under a study. My research study will delve into identifying critical common IaaS migration patterns and information security needs during IaaS actual migration. This research shall use the findings to come up with a Secure IaaS cloud migration Model for SMEs in Kenya. This model will be tested using an IT-Teams IaaS migration software automation tool which is the output product of this research. This automation tool will later be used to ease the process of application Rehosting from on-premise to IaaS Cloud platforms.

1.3. Research Objectives

The overall objective is to identify processes for secure IaaS cloud migration and use the findings to develop and automate a migration model

1. To identify common key processes undertaken when migrating systems from on-premise to IaaS cloud.
2. To identify key security policies required in conducting a secure IaaS cloud migration process
- 3.To identify the critical team attributes needed to effect a complete IaaS migration
4. To develop a secure IaaS migration model and an automation tool.

5. To test and evaluate the generated model using the developed tool.

1.4. Research Questions

1. What are the common key processes undertaken when performing IaaS cloud migration?
2. What are the security vulnerabilities that can be mitigated during migration?
3. What are the critical team attributes required to effect a complete migration?
4. Which model can be used to impart technical skills necessary during IaaS cloud migration?
5. Which automation tool can best ease the actual IaaS migration process?

1.5. Research Significance

An increase in acceptance of cloud adoption has seen several papers explore the requirements and influences of the cloud. Some have focused on possibilities of running business systems on cloud platforms while others have sensitized the need for further research works on the actual cloud migration process with a strong need to incorporate security and enhance the capacity of the various IT skill-sets that collaborate in Rehosting systems to the cloud. The actual process of migrating systems to the IaaS clouds should be right from the initialization to the end. With complexities and challenges experienced during IaaS cloud migration, common migration patterns could be established within a given set of enterprises under a study. For a cloud migration process, having the right composition of expertise skill, and implementing the right technologies are major concerns in undertaking a migration project (Claus,2013). As proposed by Yousif (2016) , SMEs could gradually build IT expertise skill required for migration by practicing with small system components over time to develop IT technical skills needed to migrate and Rehost more vital systems in future. IT skills team collaboration has also been cited as an essential focus for future IaaS Cloud migration research works by David (2013) work. As proposed by David (2013), Andricopulous (2013) , Claus (2013) and Yousif (2016) works, IaaS Cloud migration studies should incorporate aspects of security during the migration process and include studies to build migration expatriate skills required to execute various tasks in an actual migration process.

1.6. Definition of Most Significant Terms

SME: Any business whose number of employees fall under a particular limitation. In the United Kingdom, it's a business with below 250 employees. In Kenya, it's a business with not more than 150 employees.

IaaS: Cloud computing offering that offers virtualized computing resources in terms of storage, servers, networks and other devices to its customers on pay per use basis.

IT: A general term for anything related to computing technology.

SOA: A framework widely used in computing technology that views various computing elements as services in huge infrastructure.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

This chapter presents a review of theories and models in the existing knowledge of study on cloud IaaS cloud migration. It is a summary of studies done by past scholars in their contribution to the field of cloud computing. This review was sourced from theoretical and empirical literature sources relevant for this undertaking. This chapter provides evidence of existing literature in the body of knowledge related to cloud migration and further confirms the need to undertake this research study (Kofod-Petersen, 2014). This chapter gives an insight into what other scholars have done concerning this study, what models they came up with, and what recommendations they made about the IaaS cloud migration. A conceptual model is also derived as summary of insights presented in this chapter

2.2. Cloud Computing in Enterprises

In businesses, the use of cloud technology is very significant since it helps the company upscale its technology capabilities, cut down on IT infrastructure cost and extends access to companies' data. In any organisation, data is the most valuable asset since it helps in virtually all activities and operations of the business. In the recent times, cloud computing is increasingly gaining prominence and popularity each day. PC Magazine says that cloud computing was making around \$200 billion a year in 2012 with the prospects of making up to \$270 billion in 2020. According to AMI Partner (2014), SMEs have invested over \$100 billion in cloud computing which shows the increased uptake of the cloud technology. Organisations currently have continued to grow their use of the cloud platform, with many more migrating to use this platform. Cloud services enable the enterprises to use only the resources they need which make them relinquish any unnecessary resources which in a way puts the firm in a position of efficient allocation and use of its resources. This is a cost-effective measure which is a great way is the advantage of cloud computing and which has seen its uptake by many SMEs.

According to insights from SAP (2015) study of the adoption of cloud computing and Oxford Economics, 69% of the businesses expect to make cloud investments that are visible in three years as they move to the cloud platform. Presently 32% are using the cloud to streamline their supply chain, and enterprises predict that this figure will be on the rise to 56% in the next three years.

Already 44% of the businesses use cloud computing to bring on board new business models with the projection of 55% in three years' time (Columbus, 2015). These figures are very articulate on the significance of cloud in bringing benefits to the business. SaaS (software as a service) comes out as a delivery paradigm that is winning while the Infrastructure as a service (IaaS) is facing an evolution that is troublesome due to reduced target and the lack of expertise. For most of the portfolio of applications, rationalization is a big challenge when it comes to migrating the applications to the cloud (Merryman, 2015).

Migration to the cloud for enterprises poses different challenges, and this makes the private cloud to be the most adopted since it offers a smooth transition from the traditional on-premise model to the cloud infrastructure and offers the Internal IT more control over its data security (David G. Rosado,2012). In retrospective, the community cloud seems to be the most sophisticated hence it is an unusual choice for many businesses Again the issue of staffing for cloud migration becomes a hindrance to most SMEs which raises the need to have experts who create a smooth flowing migration. The cloud skills-gap and staffing have been cited as major blocks to cloud migration. As Tavana and Puranam, (2014) put it, "It is difficult for SMEs to find the right skills and afford competitive pay scales" in cloud computing staffing. Hiring and training technical staff in SMEs have been proposed as workaround solutions to solving the pertinent cloud skills-gap problem. Training has been preferred to hiring in Yousif (2016) cloud skills solution; according to this work, technical staff within SMEs could practice by migrating small systems components to the cloud over time to gain experience in performing large systems cloud migration in future. Again the introduction of an IaaS IT-team automation tool becomes a viable research study in continuation of these previous works based on the recommendations of the above-cited works by Tavana and Puranam, (2014) and Yousif(2016). Introduction of an automation tool and incorporation of security in the derived model of this research, therefore, presents an additional uniqueness that contributes to the existing body of knowledge and potentially addresses the IaaS skills-gap in SMEs.

2.3. Security in Cloud Migration

Cloud computing offers profound benefits to the IT industry and continues to redefine the operations of Information technology in businesses. In this regard, the benefits of adopting the cloud include reduced IT services interruptions, reduced software maintenance, and centralized management of security. The cloud computing reference architecture, on the other hand, establishes an analysis of standards for services portability, safety, and interoperability. Most security risks posed by the cloud are like other IT security concerns, but additional risks may be specific to the type and operation of a particular cloud. The four major security issues listed by the Cloud security alliance include shared technology issues, exploitation from malicious insiders, Data Loss or leakage, service hijacking, and insecure interfaces or APIs. In IaaS responsibility for the shared technology is on the Cloud Providers (Stallings, 2016).

Migration to the cloud technology poses many security risks to the applications, and so there should be enough measures to ensure no loss of applications or data. With the lack of personnel with technical capabilities to carry out successful migration in the SMEs, the risk to the applications is higher which needs more stringent security measures. According to Andricopulous (2013), any safety risk during migration can be reduced through the process of migration, choice of provider and standards of security implemented during the process of migration. The Cloud adopters need to understand the different security risks that the process of migration faces so that they can implement the best internal measures to mitigate each of these risks(KPMG,2014). When it comes to cloud technology, security is considered to be the biggest issue of concern, and many businesses view security as the primary cause as to why they do not adopt the technology (Monika and Kalpana, 2016). It is very illogical to invest in the best technology which will not meet the intended purpose of its adoption.

Having adopted the cloud, an organisation may grant access credentials and entrust specific employees with the management of the cloud resource. However, some employees may exploit this trust in compromising and attacking the company's cloud. Stolen credentials remain a top favorite in compromising the cloud security. Having the access credentials, attackers access critical data hosted on the cloud which formulates a basis for cloud services hijacking. At times, the adopters fail to review and check the security demarcation points in their service level agreements with the IaaS provider. Adopters will, therefore, deploy applications with a thought that all is

secure without observing the set procedures and policies of the Cloud service provider. This introduces a vulnerable for exploit by an attacker. With these and other vulnerabilities introduced with the adoption of the cloud, there is a need for IT professions to implement preventive and countermeasures that suppress and prevent potential attacks. An occurrence of security attack compromises on data in the form of deletion, alteration or eavesdropping. Removal or modification could cripple an entire organization in the absence of data backups. Loss or exposure of an encryption key could lead to massive data loss, and unauthorized access could gain access to highly sensitive data (Stallings, 2016).

The Cloud security Alliance describes cloud security as a set of tasks and provisions with defined categories of services. These include identity and access management, web security, Encryption and cryptographic schemes, Network security, Intrusion prevention and control, Disaster recovery, Email security, data loss prevention and continuous security assessments. Cloud Identity access management (IAM) are efforts that ensure system entities and people are granted rightful access to resources on the cloud platform. This combines access control and authentication of system services while accessing the cloud. Data Loss prevention includes measures of protecting and verifying data security either on the hosted data or in exchange to and from the cloud environment. Web security measures combine any efforts geared towards the safe use of the web environment. Intrusion management entails activities that identify any unauthorized access to the system. Security information and event management provide for the gathering of logs and events from cloud environment aspects which is later analyzed to identify activities that may need intervention or any other action. Encryption, on the other hand, is pervasive services that operate across large computing environments to enforce security of the cloud platform. Encryption could cut across key management, application encryption, data content access and virtual private networks (Stallings, 2016).

Enforcing these security measures during migration will also make the technology safe for the users, and this gives them high confidence about the safety of their data not being prone to any hacks which may compromise the business (Khajeh, Greenwood, and Sommerville,2010). SMEs have low expertise in using the cloud technology, and so they should make sure they follow the basic principles of software security which will help minimize any risks ((Khan and Al-Yasiri, 2015). Enterprises are developing a cloud strategy which composes security guidance on

acceptable uses for SaaS, PaaS, and IaaS. Cloud providers offer varying security measures to their customers mostly through giving pre-built security controls to reduce the risk and make migration easy. These control, however, should be configured and controlled by applications and this is a critical security concern that should be addressed during migration. (Barker, 2016).

2.4. Migration to the cloud -Case Kenya

Despite Kenya being a developing country, it has made tremendous steps in embracing the use of cloud technology. According to Kenya Communications Authority 2016, Kenya has experienced at least 58206 new migrations to the cloud which depicts a positive uptake of cloud technology by businesses both SMEs and large scale. As (Mokelena,2014) puts it, most companies using noncore in-house computer systems such as customer relations and email systems will continue to migrate to cloud solutions as they seek to keep testing the reliability of cloud technology (Jackson, 2014). With the availability of fast cable Internet in Kenya, use of cloud technology is enhanced which is helping companies especially SMEs take their place in the global digital economy. For SMEs who do not afford fast and reliable internet, their operations are harbored by increased IT operation costs. SEACOM business is leveraging on its scalable and abundant capacity on the undersea cable and IP-MPLS continent-wide network as well as the capabilities of cloud technology to enable corporates and SMEs in East Africa smoothly migrate to the cloud (CIO East Africa, 2016). Cloud services demand has increased in the last three years propelled by the growing demand for Digital content in Kenya. The demand for digital services has pushed the use of cloud technology driven by the need for digital services which are affordable (Wanjiku, 2017).

As Sullivan (2013) describes, markets of cloud computing in Kenya and South Africa will more than double to \$288million in 2018 up from \$114.6 million achieved in 2013 and availability of Internet bandwidth connectivity influences this. This report by Sullivan & Frost on cloud marketing in Kenya and South Africa said that increased availability and use of the bandwidth connectivity available in these two countries had created platforms which have led to the development of cloud computing. In most SMEs, in Kenya, complexities of the cloud, mistrust in third parties and security wariness are discouraging them from increasing use of cloud technology. As observed by Makena (2014), though ICT personnel's in Kenya possessed adequate understanding in operations of computer networks and databases, cloud computing skills of actual

cloud migrating and systems deployments to the cloud was a missing component requiring future research attention.

2.5. SOA in Cloud Migration

SOA and cloud computing are terms which complement each other and in this complementation comes their relation to technology. However, without SOA, SMEs and other businesses will face challenges in using cloud computing due to the lack of an architectural foundation that is strong (Ayman Massoud, 2015). Over time these two are assuming more roles that are prominent in big organizations with the aim of cost reduction and efficiency in the business. SOA is an architectural design for the transformation of the distributed systems which changes resources into services of software (Zhao et al ,2014). Adoption of SOA presently improves how technology can meet the business in the future. It is an architecture which is dominant and which will shape how organizations both big and small carry out their operations (Amorim, 2014). According to (Lewis, Litoiu, and Ionita, 2013), business departments are changing the efficient functioning of the firm from ad hoc to satisfy the requirement of change. For the process integration, it means bringing on board a cloud solution into the flow of the process basing it on data objects that are common. Therefore, there is the use of concepts of SOA like the enterprise business objects which contain different data. SOA tries to streamline the integration in the whole system by providing architecture components described and modeled in a consistent fashion(Nicholas,2013).

Cloud services focus on turning IT computing aspects stack into commodities which can get sourced from the cloud providers. Cloud computing is a broader SOA and covers the whole hardware stack through the layer software systems. SOA even though not conceptually restricted to software is mostly implemented as software services or as components as exemplified by the service standards of the web used in the majority of the implementations (Raines, 2009). The SOA framework will be referenced to provide solutions in solving the complexities of an IaaS cloud migration envisaged in this research study.

2.6. Existing IaaS Cloud Migration models

Infrastructure-as-a-Service (IaaS) is one of the primary offerings in cloud computing. An IaaS offering provides customers with remotely accessible servers, networks, and storage to host, run systems and store own data on a provider's cloud. IaaS is provisioned on-demand and managed remotely over the Internet (Nabeel Khan,2015). In IaaS cloud environment, the key roles include the service provider and the service consumer whereby the IaaS consumer requires a secure low-cost, and flexible platform to use. In the IaaS cloud, the consumers do not have access and control of the underlying physical cloud infrastructure. However, IaaS grants its customer an exclusive authority of storage, systems, applications and network components as paid for by the consumer. A consumer is responsible for security controls relating to their hosted systems e.g., the Operating system, deployed applications and data. An IaaS provider in return guarantees the underlying hardware security. An IaaS provider offers resources that are highly scalable and adjustable on demand, and this makes IaaS suitable for workloads which are temporary or which can change without expectations (Rouse, Subashini 2013). With IaaS, businesses can move their traditional international IT infrastructure to an outsourced business arrangement. IaaS have other benefits like low cost and increased IT security controls over hosted systems which makes it suitable for SMEs uptake (Bhardwaj, Jain and Jain, 2013).

Previous research works have made attempts to reduce complexities involved in an IaaS cloud migration. Binz (2013) IaaS model presented the IaaS migration as a process of establishing the appropriate provider to migrate to and making a decision to either relocate some of the system components to the cloud one-at-a-time or migrating all system components at once. Migrating all elements at once to the cloud is most favorite since it incorporates system functionalities migration, business process focus, and logic maintenance. (JF Zhao 2014).

According to Sabiri (2015) , Binz(2013) model focussed on software stack migration as opposed to migrated services functionalities and the complete architecture compatibility to the cloud environment. A SMEs SOA migration model by Nicholas(2013) decomposed business processes into data and services that need to be migrated to the IaaS cloud, and this model further defined the SME business systems that could be migrated and their cloud fitness. However, the model focus was on what could be migrated and not how they would be migrated.

Sabiri(2015) Metamodel leveraged on Binz(2013) model and went ahead to define the process of identifying the objectives to be achieved with a cloud migration process, identifying architectural components of the application and identifying physical resources with their physical assets utilization needs. This model presented the possibilities of implementation on IaaS cloud environment. The actual IaaS migration, implementation and security components are missing in this work. As Adricopulous(2013) puts it, "security, a key component in IaaS migration process," was missing in previous IaaS cloud research work.

Cisco(2011) model breaks down an actual IaaS migration process into three processes of:

- i) Identification of the business and technical requirements for migration.
- ii) Reviewing the application architecture and environment needs.
- iii) Formulation of a work plan and schedule to guide the actual migration.

In conducting the actual migration process, Cisco(2011) model recommends invocation of Cisco professional migration experts to perform the actual migration. As observed by Nicholas(2013) , invocation of specialist IaaS migration professional consultants attracted enormous costs which further discourage SMEs from Rehosting their existing systems to the IaaS clouds.

Cloud infrastructure costs having deployed a company's system to an IaaS cloud was the focus of Kahjeh(2012) research study. This research work described a case study of migrating an Enterprise IT System to IaaS where the company in focus achieved a 37% annual reduced cost by deploying its system to the IaaS cloud compared to if it had implemented the same system in its Internal IT infrastructure. This work recognized the need for IT-team collaboration in the success of IaaS cloud migration and administration. The output of Khajeh's research work was a tool that aided in decision making while adopting the IaaS Cloud from the perspective of business' development team, technical team, support team, and Project management team. A review of this work by David G.Rosado(2013) notes that though Kahjeh's work presents a useful tool in decision making across various teams in a company, this work did not provide any actual migration process for moving legacy applications to IaaS clouds nor steps of configuring and deploying systems on the IaaS cloud. IaaS actual migration skills-gap have been described as an inhibitor to a successful IaaS migration project. As Yousif(2016) puts it , there exist an expertise skill gap within SMEs on capabilities of migrating systems to IaaS clouds, this has further been enforced in Microsoft

whitepaper(2016) which identifies cloud migration skills as a future IT profession skill for global IT Job acquisition markets. Yousif (2016) works attribute IaaS migration skills gap to constraints in high costs of having skilled IT personnel within SMEs. This work proposes a continuous enhancement of ICT IaaS migration skills by SMEs through practice with small IaaS services migration over time to equip IT-teams with necessary skills needed for quality. As Adricopulous(2013) puts it, "security a key component in IaaS migration process," was missing in Kahjeh's work. Adricopulous(2013) further enforced the need for a future research tool that guides IT technicians in migrating the legacy application to the IaaS cloud.

This research work is unique as it is a continuation of David (2013), Andricopulous (2013), Claus (2013) and Yousif (2016) works on IaaS Cloud migration studies. This study intends to research on a secure IaaS cloud migration model to be tested through an IT technicians' automation tool as the output of this research. This research focus is on identifying patterns in SMEs Rehosting systems to the IaaS cloud, identifying information security needs during actual IaaS cloud migration and developing a tool to impact needed IT-team's skills while conducting an IaaS actual migration process.

2.7. Cloud Automation Tools

Cloud automation tools enable automation of complex processes in cloud environment management. Cloud automation tools are used to enforce security, scalability, repeatability, and reliability of the cloud computing environment. They help ease processes in the deployment of services, allocation of resources and management of tasks on the cloud. The difference between automation tools and Virtual Machines in the cloud environment is their ability to automate processes involved in the cloud environment. On the other hand, virtual machines provide the ability to share computing resources on the cloud. While virtual machine in IaaS gives the ability to provision services and applications to the cloud, they do not provide crucial information on cloud resources management.

Cloud automation tools have been a significant focus and output tools in several research works in the past. Zhan and Shang (2014) developed a tool for deployment of operating systems to the Open stack cloud computing platform. Zhan and Shang (2014) mission were in easing the process of deploying multiple operating systems on the cloud. In this research work output, a graphical user interface was provided to aid users in implementing various operating systems on opens stack

platform without expert knowledge of the cloud. This study by Zhan and Shang (2014) introduces a possibility of automating the execution of a process on the cloud. With this tool, users were able to perform cloud processes of deployment of operating systems in the cloud without the requirement of expert knowledge. Callanan et al., (2016) paper discussed the challenges faced while migrating the application to the cloud and provided an application environment framework for automating the migration of infrastructure. However, this research work by Callanan et al., (2016) did not implement the framework. Besides these research works, other cloud automation tools have been developed by infrastructure providers and scholars. These tools include terraform, habitat, cloud formation and Docker.

Docker is a cloud automation tool that is used in deploying and running services on the cloud by use of containerization. Docker presents an additional mechanism for implementing computing services to the cloud. Unlike virtual machines, Docker enables applications to share the same kernel. This tool is designed for use by system administrators and cloud adopters. From a cloud adopter's perspective, Docker provides the necessary tools needed in applications development. Docker also improves IaaS cloud flexibility and is open source. The success of Docker has seen several IaaS cloud providers develop pseudocodes for its integration to their underlying infrastructure. Some of these IaaS providers include Linode, Amazon, Digital Ocean and Go daddy.

Cloud formation tool is provided and provisioned within the AWS cloud. Cloud formation tool helps ease management of applications deployed on AWS. Cloud formation tool enables adopters to create and modify a template file on AWS that define how the cloud resource should be managed. Cloud formation stores the template file and automatically executes tasks defined in it. Therefore, cloud template files help an adopter in the management of the relationships between different tasks in the AWS cloud. Zin summary, AWS helps ease infrastructure management, reuse of infrastructure, and control of changes to Infrastructure that ensure consistency (J, Pawar and V, 2017).

Terraform is a cloud automation tool that focuses on management of cloud infrastructure as code. It is used to develop codes that implement the knowledge of performing different tasks in the cloud environment. It is best used in configuring, managing and versioning the cloud through codes. In terraform, the cloud infrastructure is defined using the syntax of code. The codes are used by

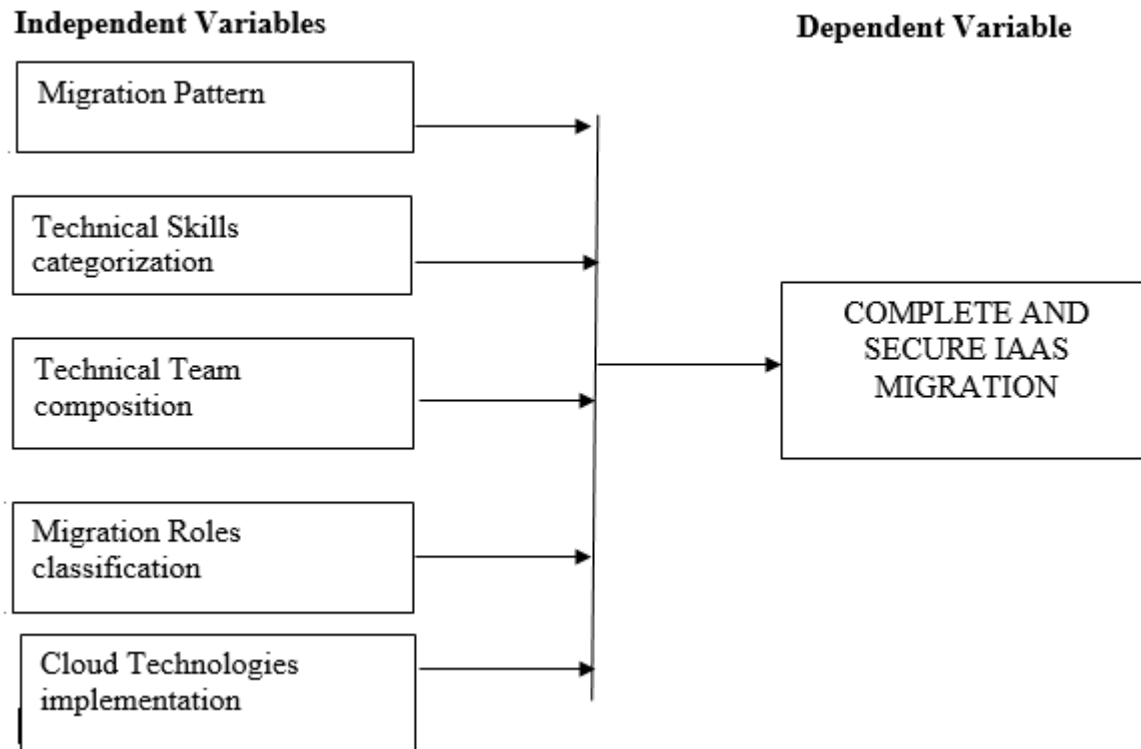
terraform in formulating execution plans with schedules and procedures. The execution plan is then effected by the tool.

Habitat is a cloud automation tool that focusses on an application and how it adapts to the cloud environment. Habitat packages an application and the context in which it runs on. It enables the adopter to focus on the cloud migration process and the features that are needed to be added or reconfigured with a cloud migration. A habitat application is compatible to containerized, bare metal or PaaS environments. A habitat application is, therefore, an independent environment (J, Pawar and V, 2017).

The focus of this research is in the development and automation of an IaaS cloud migration model for SMEs in Kenya. This research output tool automates the process of IaaS migration by the IT team in an organization. IT teams in organizations possess different skills essential in performing a complete IaaS Migration process. These skills include systems development, infrastructure management, Network administration, and Cybersecurity (Makena,2014).

Unlike other automation tools reviewed by this study, the output tool of this research will address actual migration skills gap in performing an IaaS migration. It can, therefore, be best described as "an IaaS cloud automation tool with an adopter in mind." This tool will aggregate IT technical skills in SMEs to effect a successful IaaS cloud migration. Every skillset required in the actual migration process were identified and accorded a role to play in effecting the IaaS migration. A relationship between designated migration tasks and cloud security technologies were matched to a user role in the automation tool. The functions identified were be used to develop and implement user privileges on the automation tool. Having been assigned a role and authorized to effect a defined IaaS migration task in the automation tool, a user was guided on the hands-on skills required and processes in the actual IaaS migration. Having effected an assigned role, a user will check out or await a further process demanding their attention. This will continue until a successful migration has been effected. This tool will be implemented in PHP and MySQL and made available online for testing and use. It is crucial also to note that the automation tool envisaged in this research will have no bias or prevalence of any existing IaaS provider.

2.8. Conceptual Framework



Source: Author (2017)

2.8.1 Migration Pattern: This presents a common step to step approach of conducting the IaaS migration. A solid pattern ensures consistency and effectiveness in performing the migration process. The patterns identified in this study is crucial in easing the migration process. The migration pattern also presents a simplification of applications deployment complexities and provides a basis for critique or reference by future scholars of a similar discipline.

2.8.2 Technical Skills Categorization: Categorization is a measure used to identify the primary entities in the technical team that may be engaged during the actual migration. These entities are crucial during the migration process as they form the available skillsets for use in the actual migration. Their categorization helps in identification of comfort levels in effecting the migration, formation of essential knowledge pool in an organization that is trusted upon to conduct the

migration process, establishes a needed synergy between the migration task and its effector and provides a basis for classification of roles.

2.8.3 Technical Team Composition: Having the right mix of the technical characters in an organization is critical in conducting the IaaS cloud migration. This is because the technical components of an organization's team are used to affect the process. A cloud migration process, on the other hand, provides an opportunity for collaboration among the members of the technical team to start and accomplish the services migration to the IaaS cloud chosen.

2.8.4 Migration Roles Classification: This entails the establishment of a relationship between the previous two variables of categorization and composition. This means that a single migration task will be assigned to a member of the technical team in an identified category. Classification defines an arrangement of technical entities based on their categorization and requirements of the migration tasks. Therefore, an entity either is or is not required or responsible for effecting a particular task of the IaaS Cloud migration process.

2.8.5 Cloud Technologies implementation: A cloud migration process entails migration of the applications and corresponding technologies that adhere to the organization's policies. These technologies could be in the form of cloud administration requirements or cloud security implementations. Concerning security, these technologies could be access control implementations, identity management, data privacy, non-repudiation enforcements, or integrity implementations.

CHAPTER THREE

METHODOLOGY

3.1. Introduction

This chapter presents the elaborate phases and stages used to conduct the research study. This research collects primary and secondary data from various organizations who have undertaken the activities of moving computing systems to the IaaS cloud. The primary goal is to understand the process and patterns of migration and to develop a prototype for IaaS cloud migration. In doing so, this research further describes the sources of data used, the population of the study and the sampling techniques chosen in identifying the sample size. Attention is paid to understanding the individual participants including their opinions and perspectives in the entire actual migration process of Rehosting computing systems to the IaaS cloud.

3.2. Research Design

A Qualitative research's primary aim is in conducting a study that entirely involves discovery and demystifying models present in a natural setting. A qualitative research design is powerful in enabling the researcher to source a high level of understanding of the happenings of the actual experiences of the research population. However, qualitative research methods recognize a need for the researcher position and their impact in shaping the research questions, data collection, data analysis and results reporting. For these reasons, it's paramount to keenly identify the right research population and target population that produces the most accurate findings of qualitative research (Oun and Bach, 2014).

In the fulfilment of its intended goal, qualitative research designs offer five areas of choice to the researcher. These areas are by use of case study, ethnography study, phenomenological study, grounded theory study and content analysis. Ethnography studies differ in a case study approach as it studies the entire group as opposed to the involved individuals themselves. Grounded theory ultimate goal is in development of new methods of science. Phenomenological studies are aimed at understanding experiences of the respondents in conducting a particular event by interviewing the research population. Content analysis studies, on the other hand, is a systemic examination of

a focussed organization communication content to derive patterns or biases (Austin and Sutton, 2014).

A case study approach explores the more profound understanding of an event or process by examining one or more individuals. It intends to generate a deeper understanding of little-known processes or poorly understood procedures in science. This study's aims at understanding the various tasks and common patterns during IaaS migration by examining organizations and individuals who conducted a successful migration in the past. A case study approach was chosen as it provides the best method that promises an achievement of this study's intended objectives and within the required timelines. The nature of this research design is through the conduct of naturalistic inquiries in real scenarios where Systems migration have previously been performed to an IaaS Cloud with the aim of identifying past IaaS migration patterns from vital technical persons that prior undertook the process (Oun and Bach, 2014).

A research design is used to guide the execution of the research process. Research designs could be causal research design, exploratory research design, and descriptive design. The causal research design main aim is in the establishment of a cause and its effect. Exploratory design n is meant to derive insights on the occurrence of events, and descriptive research designs determine the frequency of the happening of a defined study phenomenon. Descriptive approaches are invoked in conducting this research. The motivation for choosing descriptive method is its ability to collect data from large samples cheaply and efficiently fast. Descriptive approaches offer potent means to incorporate human experiences into research which is a useful component that this study seeks to delve in. Also, descriptive approaches provide much-needed flexibility by a researcher to view the study in a more prominent and broad perspective (Field, Miles and Field, 2014).

Reflexivity is also another aspect put into consideration in this research. Reflexivity defines a possibility of the researcher's absolute knowledge in the area of study that may affect the process of research. In controlling reflexivity, this study adopts a detached objectivity approach where the researcher maintains a perspective of independence of thought and also assumes the role of a neutral bystander within the entire research (Oun and Bach, 2014).

3.3. Population Sampling

Purposive sampling was used to guide the conduct of this research. Purposive sampling focusses on a particular group of respondents with specific characteristics intended by research. Purposive sampling also enables the researcher to select a target population who are willing and knowledgeable to participate in the study (Palinkas et al., 2013). In this research, the particular characteristic of the population sample was a requirement to have undertaken an IaaS migration in the past. A population is a term used to inference a group of elements which have similar characteristics. A sample is a small group that is used to represent the broader population and sampling is the process of identifying samples that correctly describe the population (Field, Miles and Field, 2014).

The population of this research was technical SMEs' employees that had previously conducted an IaaS migration. There are more than 58206 past cloud migrations in Kenya who have adopted the cloud in the capital Nairobi by the year 2016. This formed the research population of this research. Therefore at least 25 SMEs was selected. These were the sources of primary data collection in this study. These were selected on the basis of experience in migrating systems to the cloud. This selection was effected via email correspondence, phone calls to respective organizations and personal visits to the Organisations in Kenya. Secondary data was sampled from Roamtech solutions Limited-Kenya. Roamtech solutions limited is a licensed content service provider under the Communications Authority of Kenya which boasts of over ten computing systems hosted on the IaaS cloud. Roamtech solutions limited also has well-developed IT-Team skill sets that collaborate during the migration process. These skill-sets include systems development, customer service, and Infrastructure specialists. All these skills are used to effect a migration project. This company was selected on the merit of availability, the sufficiency of a well-established cloud administration technical team and consent to access useful data relevant to this study. This research sought to identify patterns in IaaS cloud migration and use the findings to develop an IaaS migration automation tool.

3.4. Data Collection

Data collection process is a crucial process in the achievement of a research study's objectives. In qualitative research methods, data collection could either be through direct interaction or indirect interaction with participants. For this research, primary data was gathered using a combination of

open-ended and closed-ended questions in the questionnaire attached in appendix 5. This was distributed to [twenty-five respondents](#) who were the target sample of research. The researched groups for this research were technicians and IT professionals in companies within Kenya who had undertaken an IaaS migration at a previous past date. Due to their limited availability, the data collection technique was primarily via the Internet. The questionnaire was distributed via survey monkey, an online survey conduction tool. Therefore, survey monkey was used as the primary data collection tool in this study.

The following were the primary sources of data sourced from the research respondents:

- The IaaS cloud providers' environments used
- The type of IaaS cloud service model used
- The process and tasks executed to Rehost systems on the IaaS clouds
- The IT technical skills needed in conducting a complete IaaS migration process
- The Best method in allocating roles to the IT technical team that performs the migration process
- Security implementations and technologies deployed in securing the adopters IaaS cloud.

Secondary data collection was carried out on Roamtech solutions Limited-Kenya, one of the 25 samples in this study. Secondary data was sourced through direct interaction from:

- Interview with the IT manager
- Interview with the Infrastructure Head
- Reviewed Existing IaaS hosted infrastructure and data centre set up
- Reviewed ongoing and future projects by the organization

For acknowledgment of the time, assistance and thoughts of participants and respondents, a copy of the research report was sent to the organizations who participated in this research and a test account for the set up in the output tool of this research for use by the participants' organizations. For all participants identified for this research, informed consent was obtained. This included

providing them with information regarding the purpose of the study, what information was required and the intention of the study.

CHAPTER FOUR

SYSTEM ANALYSIS AND DESIGN

4.1. System Specification

4.1.1 Overview

This is an automation tool used as a software assistant during an IaaS migration process. This automation tool contains the collaborative team process in effecting an IaaS migration. The key migration stages are assigned to available IT personnel before starting the migration process. Migration roles are mapped to the available technical skills and subtasks defined for execution in each migration stage. Migration stages are effected procedurally with the progress tracked for effective accountability during the migration process. Additional links to open source libraries and tools required for accomplishing set tasks and subtasks in a migration stage are provided for further explanation and steps in configuring the IaaS cloud.

4.1.2 Inputs and outputs

4.1.2.1 Inputs

The system will allow the IT technical team to be registered by the project manager using their names, their skill in the team and their email addresses. The IT technical personnel skill-composition, therefore, are the primary users of the system. Information about the systems to be migrated, the planned migration period and the specific organizations involved will also be captured. The stages, tasks, and subtasks during IaaS migration will also form additional inputs to the system. This will be provided by the automation tool.

4.1.2.2 Outputs

This is an interactive system that outputs specific information on migration stages to the users based on their roles in the IaaS migration process. The users will also be able to access additional information on effecting the tasks and subtasks in the migration process. To enable tracking of the migration process, the system will produce progress status reports which are sent to the project manager's dashboard that indicates the stage of execution during the migration process.

4.1.3 Data Management

The data in use by the automation tool is stored in a database. The system will save information that aid IaaS migration process. The User roles and the details of the company and systems being migrated shall also be stored in the database.

4.2 System Analysis

The software Engineering process chosen for this study contains three procedures of:

- i. System Design
- ii. System Development
- iii. System Testing

The main actors in the system were identified as the users in the system and their roles were mapped based on the specific skill and the stage in IaaS migration. The identified actors were the project manager, system developer, network or cloud infrastructure administrator, cybersecurity and IT support. These were the primary roles that collaborated in effecting the migration process.

4.3 System Design

The automation tool is accessed via the web interface which contains all the modules accessed by its users. The web interface comprises a link for Backend access and Frontend access. Backend access is used to access and conduct administrative tasks in the tool while frontend access is the open access module that relays information to the general public. Administrative tasks are categorised as general administrative tasks and superuser administrative tasks. General administrative tasks are affected by users undertaking an IaaS migration project while Super user administrative tasks are restricted for access when changing the components of the automation tool only.

4.3.1 Applying Use Cases

The automation tool has the following Actors and elements:

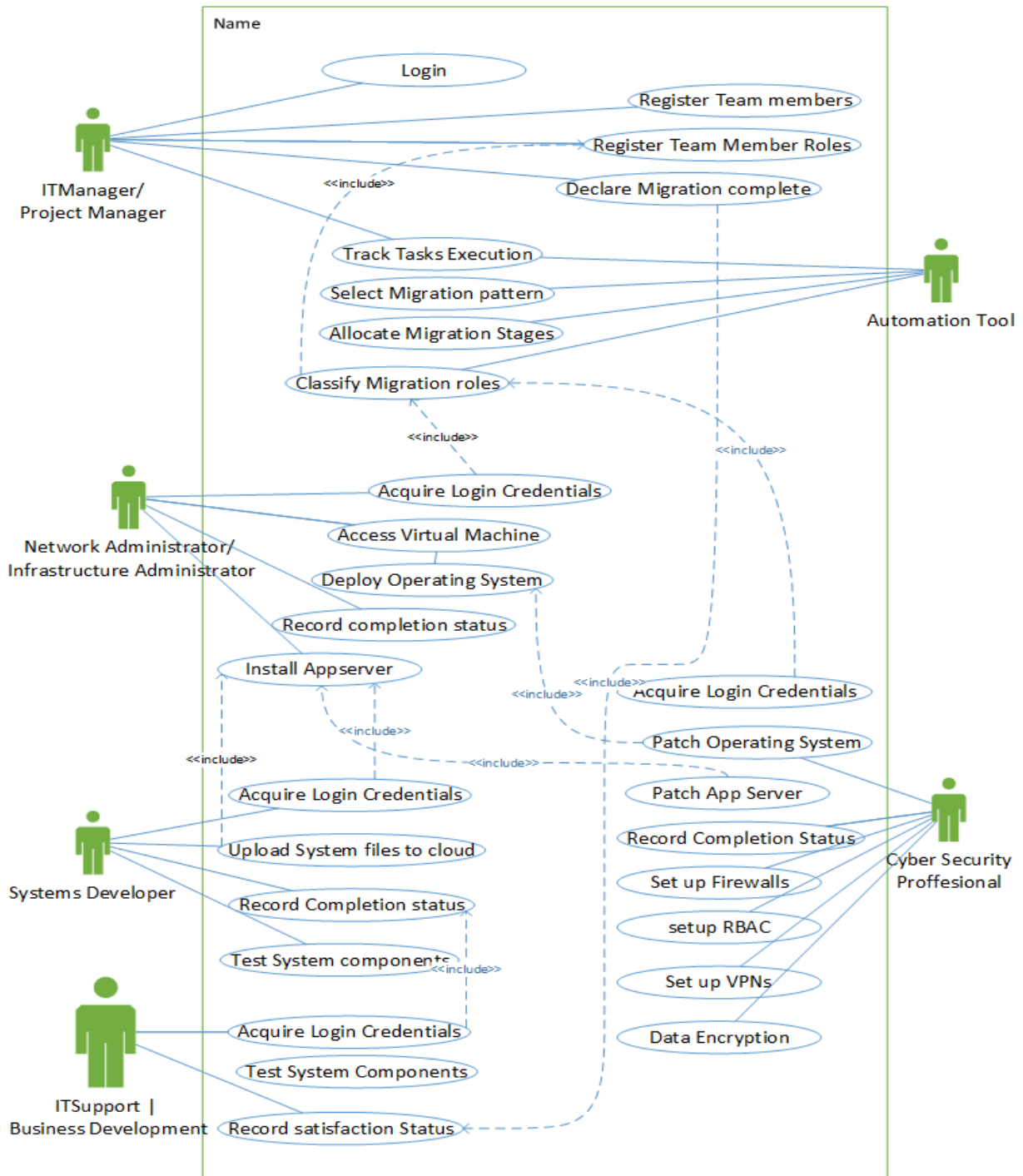


Figure 1: IaaS Automation Tool Use Case, Source: Author.

The super admin first logs in to the automation tool's administration dashboard and registers the company that wants to undertake an IaaS actual migration process. After doing this, the Super Admin registers the project manager who is the first person in the newly registered company with authorization to commission, stop or close a project. The project manager then registers all other team members who will participate in the migration project and selects a role for each team member. After team member registration, the project manager commissions and starts the migration project. Commissioning an IaaS migration project changes the project status from "Not started" to "In Progress". Each team member registered for the project is able to view the stages assigned to them and the resources needed to effect the stage even before the stage is reached. However, a team member is not able to effect a stage until all the previous stages have been executed and completed. During the execution of a particular stage, the team member responsible for that stage executes all tasks required for the stage and completion status is tracked by the automation tool. A stage is marked as complete when all required tasks for the specific stage have been completed. Upon completion of the stage, the next stage is activated, its status changes to "in progress" and the required team members sent an email prompt requiring them to log in and execute the stage. As the stages execution continues, every team member participating can see the progress of execution at any given time. After all stages have been affected, the project manager declares the migration complete and downloads documentation of all the stages and tasks completed during the IaaS migration. This document may be filled or retrieved for future system audits.

Figure 1 above indicates that the automation tool has six [main actors](#) including Network administrator, Systems developers, cybersecurity professionals, business developers, project managers and the automation tool. A Network administrator in the automation tool is allocated the migration stages of:

Stage 1: Gain access to the Virtual Machine

Stage 2: Deploy Operating system

Stage 3: Install App Server

Stage 7: Configure DNS management

A systems developer in the automation tool is allocated the migration stages of:

Stage 3: Install App Server

Stage 5: Upload system files to the cloud

Stage 8: Test system components

A cybersecurity professional in the automation tool is allocated the migration stages of:

Stage 4: Patch Operating System and App Server

Stage 6: Implement security policies

An IT support and business development professional participates in the migration stages of:

Stage 8: Test system components

A project manager in the automation tool is allocated the migration stages of:

Stage 9: Declare migration complete

The migration tool developed automates the roles allocation process of IT Technical team members during an IaaS migration project. This tool breaks down the IaaS actual migration project into nine main stages with respective tasks under them. The tool enables technical team members' collaboration while conducting the actual migration. The tool automates IaaS migration stages precedence in such a way that the IaaS migration is effected procedurally rather than ad-hoc which makes the process predictable thus further simplifying the complexities of IaaS migrations. The tool developed also automates the documentation of the IaaS migration project which in most cases is missing upon the completion of an IaaS migration project which was a concern noted during [secondary data findings](#). Further, the tool developed in this research enables tracking of the proceedings of the various tasks under the migration project and enables easier technical team's collaboration to achieve a complete IaaS migration.

4.3.2 System Architecture

The software architecture was as follows:

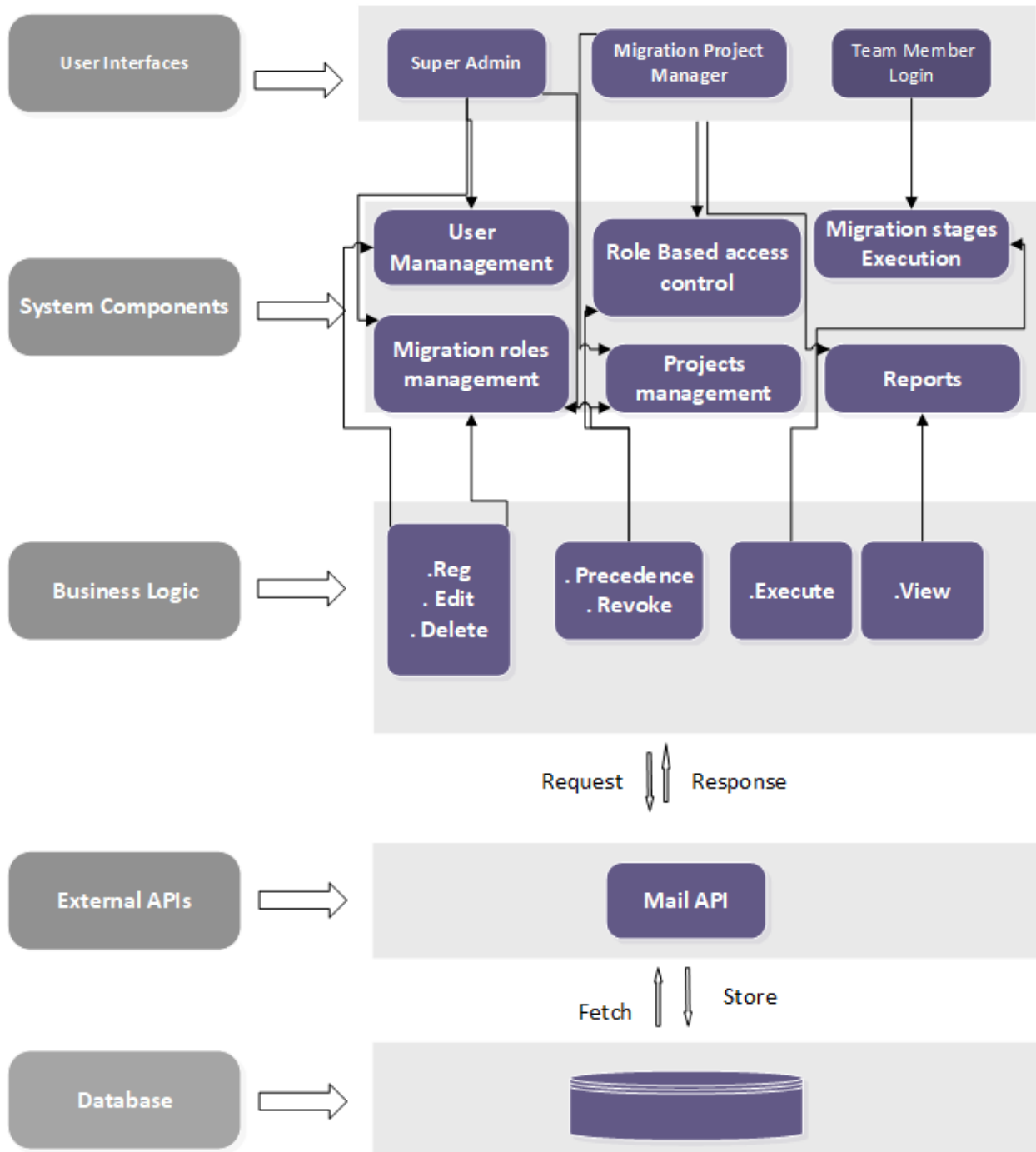


Figure 2: IaaS Automation Tool Architecture, Source: Author

Figure 2 contains the inputs in the automation tool. This tool was designed for best user experience and robustness that ensured that all components were elaborate and complete. The system components were developed using PHP. The super admin component enables the addition of critical subcomponents in the tool. This component is used to register a project manager who acts as the first contact in a new migration component.

Migration project manager component enables the project manager to access the automation tool, add team members and track the progress of the project. Project Users Login allow other project team members to log in and execute the various stages in the IaaS migration. Role-based access control ensures that only members assigned a specific role can affect a specified stage in migration. Migration stages management component enable precedence enforcement on order in execution of the set migration stages. Migration roles management component automates the classification of technical skills available to execute the project to the specific roles required in an IaaS migration. Registration component ensures successful registration, commissioning and closure of migration projects. The user management module enables addition, reassignment and deleting of system users. The system access component ensures that upon authentication, users are granted access to the specific components that are required of their role in the IaaS migration. The Business Logic Layer ensures that correct syntax, rules, and semantics are put in place to support operations of the provided components in the automation tool. The database contains the data store for all activities in the automation tool.

4.4 System Development

This section presents a framework of activities actions and tasks that were implemented in the IaaS automation tool. This was presented in Data flow diagrams of the main subprocesses contained in the tool.

Project Registration Process Flow

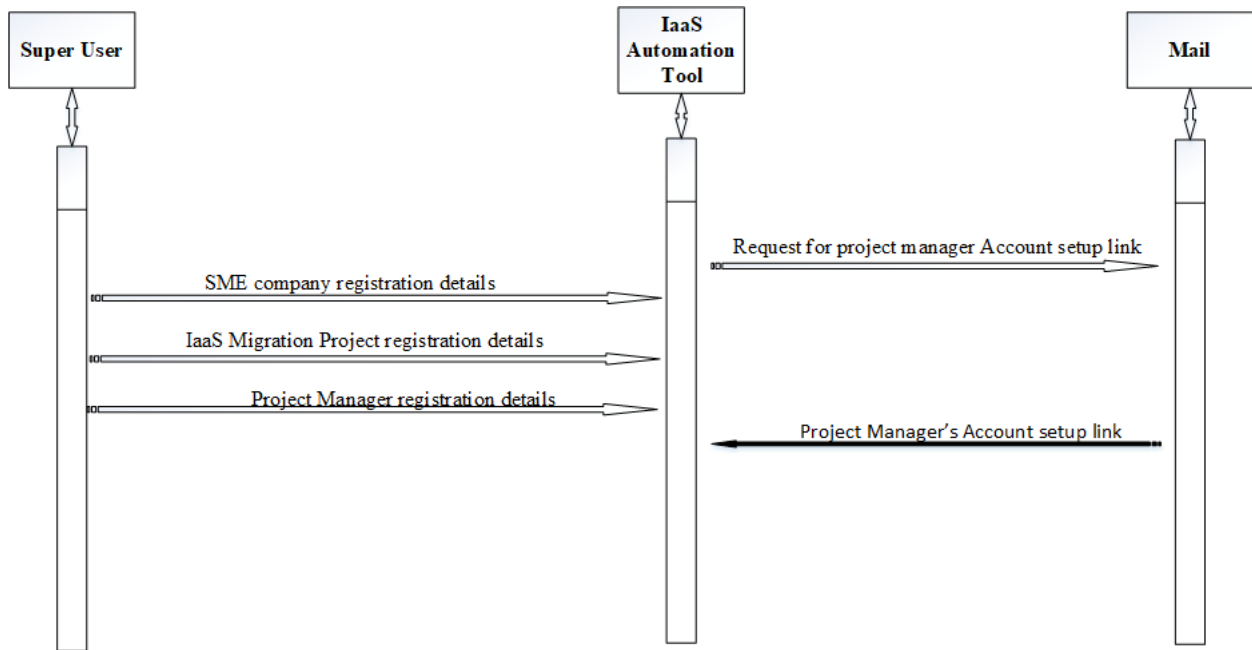


Figure 3: Registration of New Migration project, Source: Author.

The developed automation tool provides for registration of a New IaaS project by assignment of its project manager and the company registration details. This allows the super admin to define the IaaS migration project and provides a means for the project manager to receive necessary access credentials required for their initial Login.

Roles and Permissions assignment process Flow

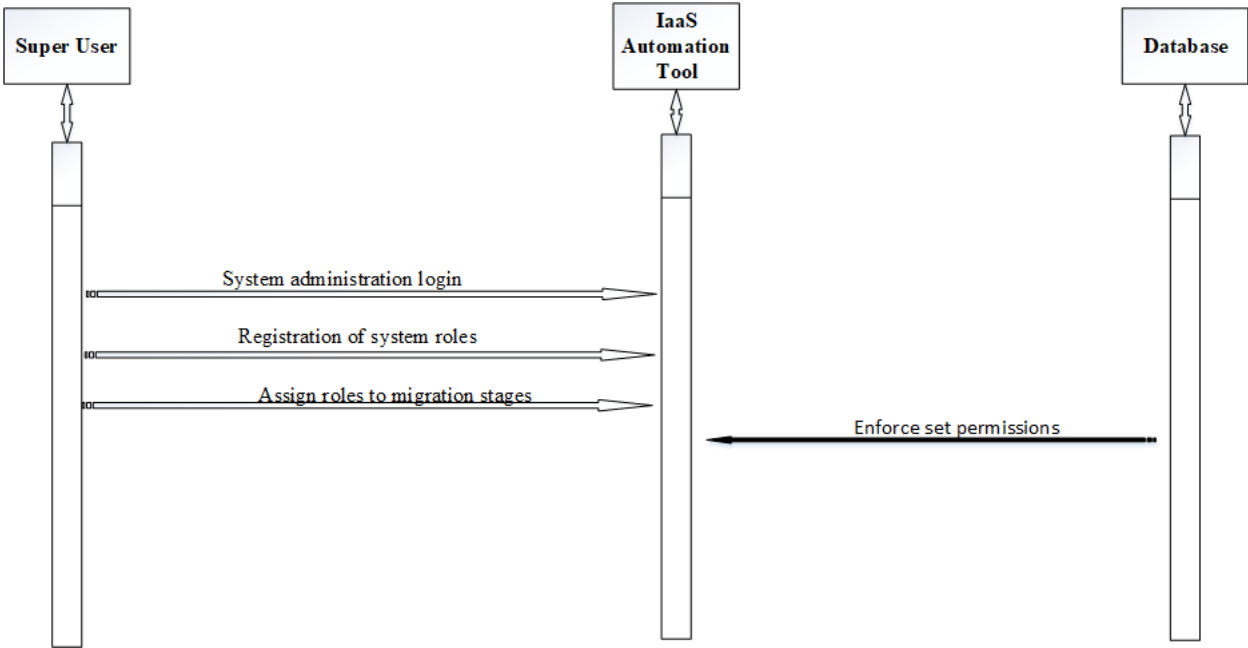


Figure 4: Roles and Permissions Assignment, Source: Author.

The IaaS automation tool provides the system administrator with authorization to register the key migration roles and assign these roles with responsibilities of affecting specific migration stages. Migration roles are the key skill sets needed to effect an IaaS migration. A holder of a migration role is assigned permissions to execute particular IaaS migration stages as defined by the system administrator.

Migration stages and tasks registration process Flow

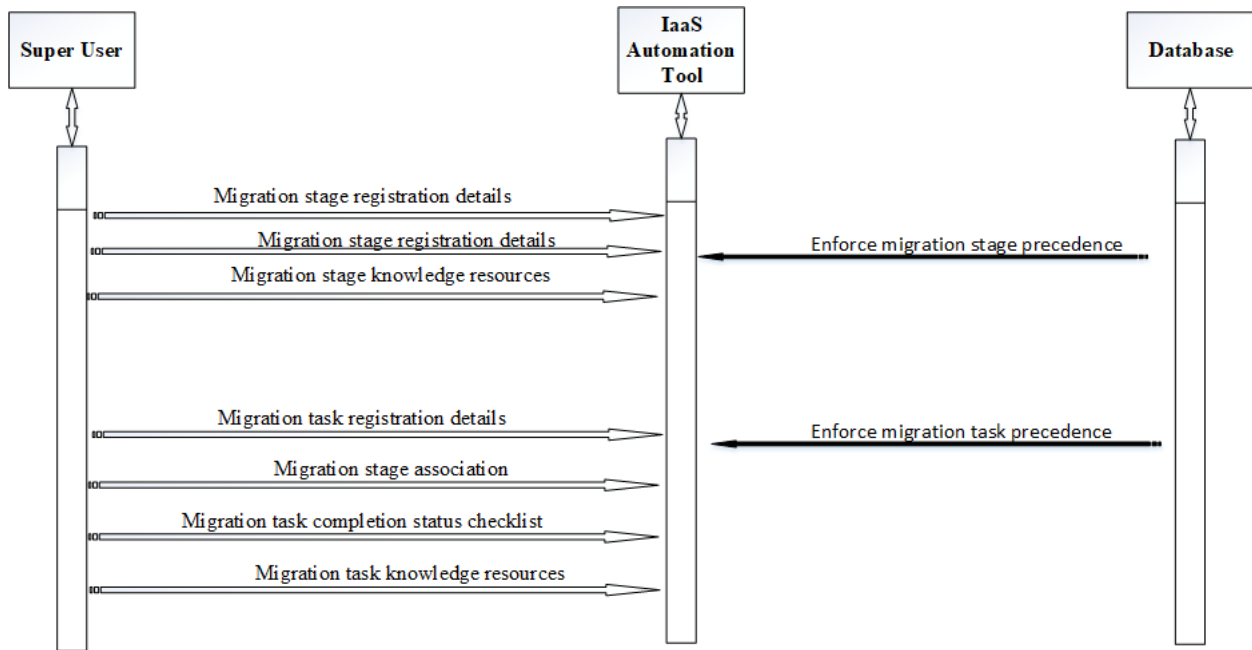


Figure 5: Migration stages and tasks definition, Source: Author.

The super system administrator reserves the rights to register the key migration stages and tasks conducted during the actual IaaS migration project. These tasks and stages are then accessible to the project manager and the teams affecting the migration process.

Team Members Registration Process Flow

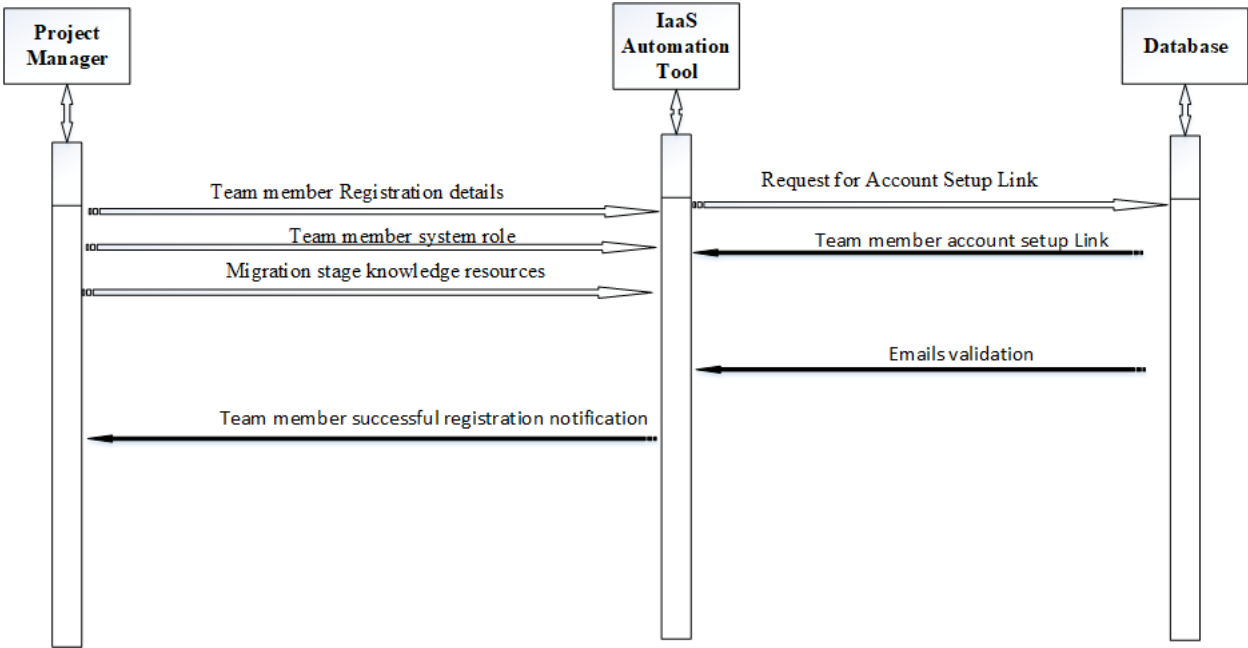


Figure 6: Registration of Team Members, Source: Author.

A team member is a holder of a migration role in the IaaS migration project. The first team member is the project manager who then creates other team members that collaborate to conduct a successful IaaS cloud migration project. The project manager also reserves the right to change and revoke permissions assigned to their team members. The Project manager can also assign a team member to new migration projects belonging to the company.

Migration stages execution Process flow

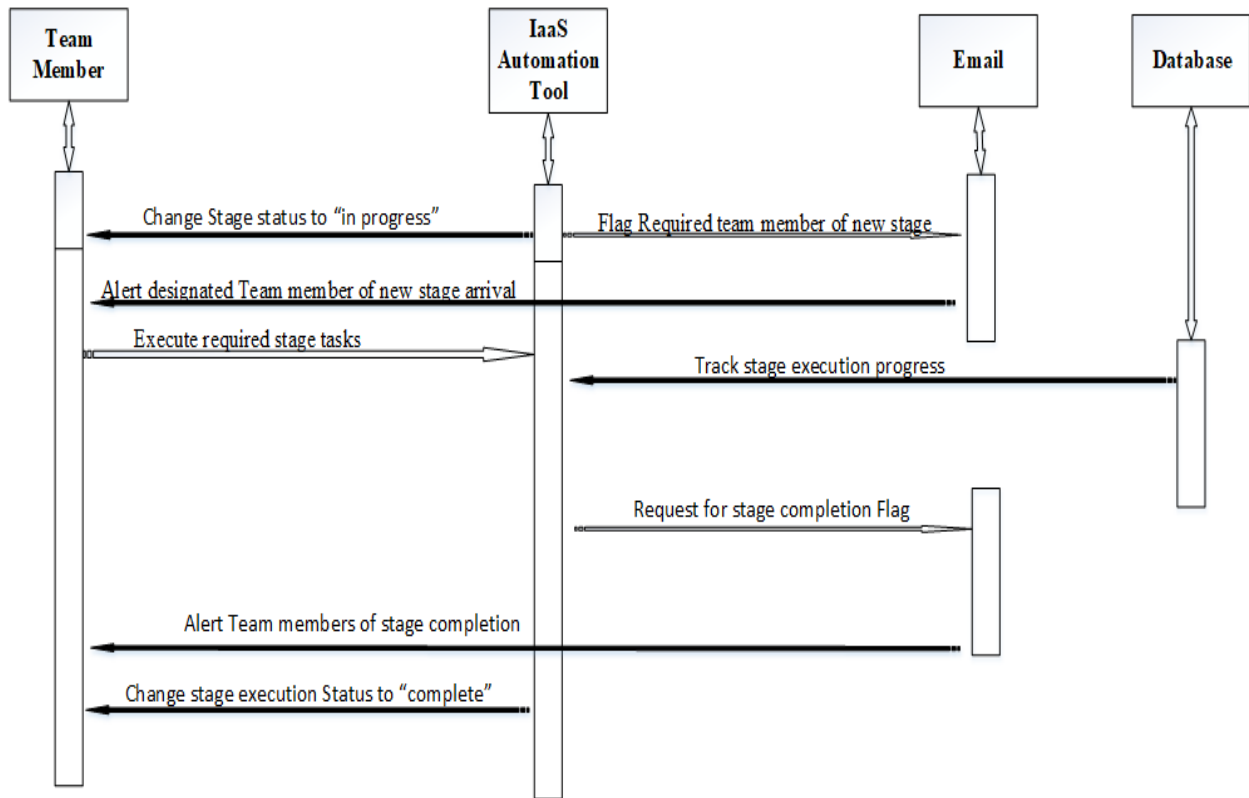


Figure 7: Migration Stages Execution, Source: Author.

A migration stage holds a single status among three other states of not started, in progress and complete. A not started stage or task has not been started as it awaits completion of a previously required stage or task completion. A stage or task in progress is one that has started but has not completed its execution. A complete task or stage has ended and all its required stages have been effected successfully. The assigned team members perform execution of tasks and migration stages during the actual IaaS migration.

Interface Development

This involved formulation of data capture interfaces and presentation forms for the web interface. The first interface captures login details during the system users' authentication. In using the system, the system user logs in to their respective dashboard via this form as shown in Figure 3 below

Figure 8: IaaS automation tool Login Page, Source: Author.

Upon successful authentication, the super admin proceeds to register the company that undertakes the Migration project. The first user in the migration project is a defined project manager who then registers other team members. A new project is registered via the interface below:

Figure 9: Registration of a new project, Source: Author.

The Super Admin registers the Stages of migration. These stages are undertaken sequentially during an IaaS Actual migration project. A stage in the migration project is registered via the interface shown below:

New Migration Stage Home

New Stage Back to All Stages

Name

Description

Order of the Stage

Which other stages must be completed first?

Stage Resources

Figure 10: Registration of a New Migration Stage, Source: Author.

Tasks to be effected at every stage of migration are registered after stages definition from the super admin dashboard. The tasks must be completed for a migration stage to be complete. Migration tasks are registered via the interface shown in Figure 6 below:

Add New Task Home

Add New Task Back to Stage

Stage: Stage 1: Gain Access to Virtual machine

Description

User Response Is user response expected?

Type of Response

Task Mandatory Task must be done for this stage to be complete?

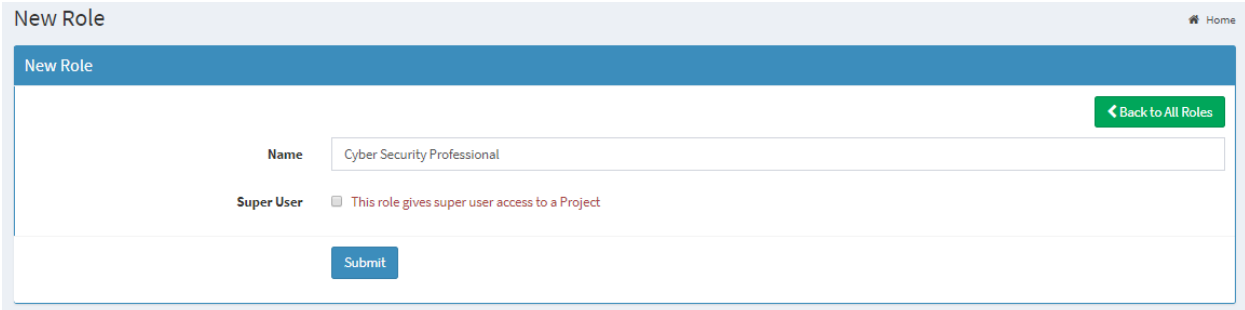
Position of the Task in this Stage

Which other tasks must be completed first?

Task Resources

Figure 11: Tasks in Migration Stages Registration, Source: Author.

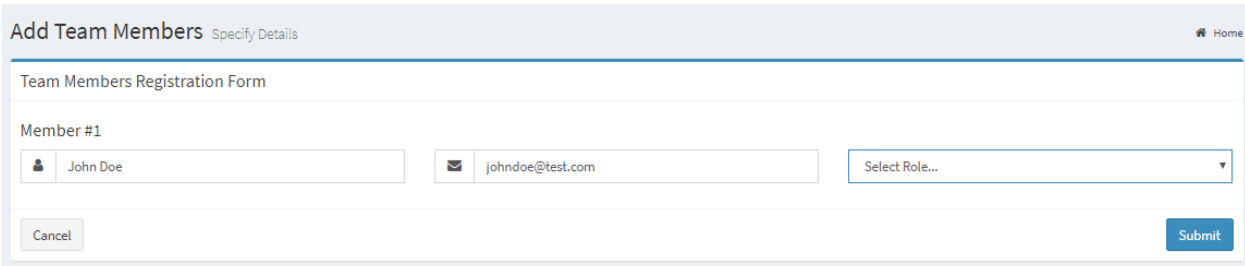
The different team members' roles are registered from the super admin dashboard. These are the different skill sets that collaborate to effect a successful IaaS migration project. System roles are registered in the Interface shown below:



The screenshot shows a web interface titled "New Role" with a breadcrumb "Home". The main content area has a blue header "New Role" and a green button "Back to All Roles". Below the header, there is a form with a "Name" field containing "Cyber Security Professional" and a "Super User" checkbox with the label "This role gives super user access to a Project". A blue "Submit" button is located at the bottom of the form.

Figure 12: Migration roles Registration, Source: Author.

The Project manager registers all other team members who collaborate to conduct an IaaS Actual migration. This is done from the Project manager's dashboard via the Interface shown below:



The screenshot shows a web interface titled "Add Team Members" with a breadcrumb "Specify Details" and a "Home" link. The main content area has a blue header "Team Members Registration Form". Below the header, there is a form with a "Member #1" section. This section contains three input fields: a name field with "John Doe", an email field with "johndoe@test.com", and a dropdown menu labeled "Select Role...". At the bottom of the form, there are "Cancel" and "Submit" buttons.

Figure 13: IaaS migration project team member Registration, Source: Author.

After registration of a new team member from the project manager's dashboard, an email with a login link is sent as shown in Figure 9 below:

PMM

Projects Migration Manager

Dear John Doe,

A new project (**Final Test**) has been allocated to you in the **Projects Migration Manager (PMM)** system. Kindly click the link below to set up your account and manage the account.

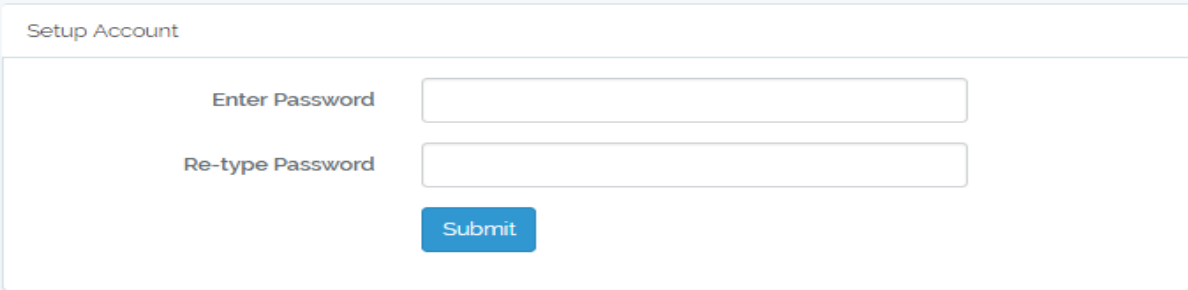
Setup Account

If you experience any issues with the link, please do not hesitate to contact the team at PMM for technical or other assistance.

Thanks,
PMM

Figure 14: New User Account Setup notification, Source: Author.

The new user created proceeds to set up their account and password from the interface shown in the interface below:



The screenshot shows a web form titled "Setup Account". It contains two input fields: "Enter Password" and "Re-type Password". Below these fields is a blue "Submit" button.

Figure 14: New User Account setup, Source: Author.

Once the Project Manager has added and defined the roles for every team member, the application will allow the users to see the stages assigned to them as well as the subtasks to be carried out in the specific stages. For example, John Doe is assigned a role of as a cybersecurity professional in the interface shown below:

My Role(s): Cyber Security Professional

Assigned Stages (2)

#1 Stage 4: Patch Operating System and App server Not Started [View More](#)

#	TASK	STATUS
1	Access Control	Not Done
2	TCP and UDP services control	Not Done
3	Security Login Banner	Not Done

#2 Stage 6: Implement Security policies Not Started [View More](#)

#	TASK	STATUS
1	Brute Force Attack Protection	Not Done
2	DDoS Attack protection	Not Done
3	Regular Backups	Not Done

Figure 15: Classification of User roles and tasks, Source: Author.

A stage or task that has not started is indicated as “Not started”. An ongoing stage or task is marked as “In progress”, a stage or task that has been completed is marked as “completed” as shown below:

Stage #1 Stage 1: Gain Access to Virtual machine In-Progress

Description: This process involves sign up and getting access to the providers cloud instance. Completion of this stage ensures that adopter has the sign in credentials to their procured cloud to be able to engage further stages in IaaS migration.

#	TASK	STATUS
1	Create account with the IaaS provider of your choice	Completed
2	Select Virtual Machine Instance and settle necessary payments	Completed
3	Acquire Cloud Login detail and gain initial Access to your IaaS Instance	Awaiting Execution

Execute

Stage #2 Stage 2: Deploy Operating System Not Started

Figure 16: Migration stages Execution, Source: Author.

4.5 System Testing

Software testing is used as a means of validating and verifying that the software developed is up to standards regarding its quality. The main aim of software testing is the identification of bugs that are resolved in this process (Yumoto, Matsuodani, and Tsuda, 2013). The procedures invoked in this stage identified any differences between the existing and the initially required conditions of the output. Any anomalies identified were resolved to ensure that the tool provided met the required quality metrics. The automation tool developed in this paper invoked both black box testing and white box testing methodologies.

4.5.1 Black box Testing

Black box testing is testing that mainly focusses on the functional testing needs of a software product. Black box testing, therefore, does not necessarily concentrate on the examination of the actual codes and logic statements of the software. Its main advantage is in the independence of its approach where the tester does not necessarily need to be the actual developer of the software. However, the examiner needs to understand the functional requirement needs invoked when the product was developed.

The automation tool was examined to ensure that its functionalities were well according to the previously generated designs. This testing was conducted on all interfaces of the automation tool. In performing this process, both functional specifications and system designs were used. A categorization metrics was developed to achieve the details in the table below. Comparison of test conditions by the number of times the changes were made to fix any bugs that may have existed was made. The following test condition list was used and the results obtained.

Feature Tested	Test Category	Spec Items	Number of Tests to Success	Score
User Login	Interface	Super User	3	Pass
		Project Manager	3	Pass
		Team Member	3	Pass
IaaS Projects Registration	Operation	Ability to register	3	Pass
Migration Stage Registration	Operation	Ability to register	3	Pass
Tasks Registration	Operation	Ability to register	3	Pass
Migration Role Registration	Operation	Ability to register	3	Pass
User Permissions Assignment	Operation	Ability to Assign, Save, Change, Delete	5	Pass
Migration Progress Status	Execution	success in Status changes	5	Pass
Tasks and Stages Precedence	Condition	Ability to enforce precedence	5	Pass
Initiation of projects	Operation	Ability to commission new projects	3	Pass
IaaS Project termination and closure	Operation	Ability to pause or terminate	3	Pass

Success rate	Percentage
3 Tests	75%
5 Tests	25%

Figure 17: Black Box testing results, Source: Author.

Figure 17 above indicates that a 75% of tested components achieved their intended functional targets within three recursive tests. A 25% of tested components achieved their intended success within five successive tests. All the components used for black box testing achieved the expected success within five tests. From the results displayed in the Figure 17 above, black box testing was completed with a 100% success rate.

The automation tool also underwent the following functionalities test phases:

Test Case	Action	Expected Result	Actual Result
Super User	Log in	Ability for Super User to login to system	Username and password authentication was successful
	Create project	Ability to register a new IaaS migration project and add a project manager	A project was registered and a project manager created for the project
	Send Email	Ability to send created project manager account setup link via email	Project manager received account set up link via email which enabled setup of password and successful login
	Migration Stages , Tasks	Ability to register migration stages and system user roles	Stages, tasks and roles created and saved successfully.

	and Roles Registration		
	Set Migration permissions	Ability to set permissions for each registered system role	Each system role was assigned permissions to execute specific stages during an IaaS migration
Project Manager	Log in	Ability for project manager to login	Successfully logged in by use of set Username and Password.
	Create Team Member, Assign migration roles	Ability to add team members and assign members roles in migration	Successfully added team members and set members role.
	Start and Close Projects	Ability to start and close a project.	Project manager successfully started and closed the project after completion.
	Report	Ability to download report on effected technologies and tasks after project completion	Project Manager downloaded reports containing all tasks executed by all members during the IaaS migration
	Track execution	Ability to view all migration stages being executed by all team members	Tasks executed by team members were visible from Project manager's dashboard
Migration Stages execution	Email Alerts	Ability for team members to receive alerts on account creation or involvement	New and required team members successfully received emails

		in their stages of execution	
	View migration progress	Ability of logged in team members to view migration progress	Team members were able to view the progress of tasks execution as stages execution continued
	Execute stages	The ability of authenticated and authorised team members to execute migration stage	Specified team members were able to execute the stage only allowed for their role
	Precedence	Ability to enforce stage and tasks precedence	Stages and tasks were only activated after completion of their antecedents
	Not started	Ability of stage or task to be marked as not started if not started	All stages and tasks not in progress were marked as "not started"
	In progress	Ability of stage or task to be marked as in progress	All stages and tasks ongoing were marked as "in progress"
	Completed	Ability of stage or task to be marked as in completed once all its requirements are met	All stages and tasks finished were marked as "completed"
IaaS Team Member	Log in	Ability of team members to login as required	Registered team members successfully logged in to their role specific dashboards

	Execute stages and tasks	Ability of registered and permission granted team members to execute tasks in their allowed stages.	Only permitted team members of a specific role were allowed rights to execute tasks in their allowed stages.
--	--------------------------	---	--

Figure 18: Automation tool Functionalities testing findings, Source: Author.

4.5.2 White Box Testing

White box testing is invoked as a means of detecting logical errors that may exist in the code. White box testing was conducted on design, application logic, and databases. Technical code walkthrough was used in conducting this process. Three technical developers were used to walk through the codes in the automation tool and pinpoint any abnormalities in the designs, application logic, API interfaces and the database. While conducting this process, the application was restructured to ensure that it met the best quality standards.

Various Metrics were used to guide the code walkthrough process. These metrics sought to determine the simplicity of codes used in the automation tool, whether all functions used in the codes were relevant to the output whereby any irrelevant functions were commented and then removed. Repeated code segments were commented, rechecked and then removed. Coding standards were enforced and all functions commented in the codes. These metrics were enforced to make sure that the style used in coding was clean and simple to understand. Appendix 6 shows the code walkthrough guide used by the experts during the white box testing process. In undertaking the white box testing process using the guide in Appendix 6 attached, experts were required to indicate their satisfaction levels of the code and logic used in developing the automation tool. The findings of the code walkthrough results are displayed in the Figure below:

<p>Expert Satisfaction Status (Not Satisfied, Satisfied, Very satisfied)</p>
--

Metric	Expert 1	Expert 2	Expert 3
standard practices have been used	Very Satisfied	Very Satisfied	Very Satisfied
The adopted style is clean and clear as a whole	Satisfied	Very Satisfied	Satisfied
Concepts applied are summarized	Satisfied	Very Satisfied	Very Satisfied
Applied functions are relevant to the overall code	Satisfied	Satisfied	Very Satisfied
Code is well segmented and commented	Satisfied	Very Satisfied	Very Satisfied
Code does not have redundant operations	Very Satisfied	Very Satisfied	Very Satisfied
			Percentile Computations
			Satisfied 33%
			Very Satisfied 67%

Figure 19: White box Testing Findings, Source: Author.

The Figure 19 above indicates that white box testing was successful with all Experts invoked expressing a 100 percent satisfactory status. With all metrics examined during white box testing, experts expressed a 67% very satisfying status of all components tested and a 33% satisfactory status on all parameters under the measure. Therefore, white box testing was successful.

4.6 System implementation

This section contains the details of the application environment in which the IaaS automation tool was developed. This section, therefore, discusses the platform and programming tools used to create the automation tool as well as the testing conducted.

4.6.1 Client Work Stations

Two client workstations were used to develop the automation tool. One workstation was used to host the complete developed components locally, and the other workstation was used for the live development of the components. The minimal requirements for the client workstations were:

Table 1 - Client workstation Features, Source: Author.

Component	Specification
Processor	Intel Core i3 CPU
Main Memory	4(GB) RAM (32-bit) or 4 GB RAM
Hard disk	500 GB
Networking	10/100
Monitor	15.5" Monitor
Internet Connection	3 Mbps
Operating System	Ubuntu 16

4.6.2 Development Server Work Stations

The Development server was used to host the system while under development locally. Only the complete and tested code was uploaded to the cloud server. The development server had the following specifications:

Table 2 - Development server workstation features, Source: Author.

Component	Specification
Processor	Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz (3 CPUs)
Main Memory	4(GB) RAM (32-bit) or 4 GB RAM
Hard disk	500 GB
Networking	10/100/1000
Monitor	15.5" Monitor

Internet Connection	3 Mbps
Operating System	Ubuntu 16

4.6.2 Hosted cloud Server Virtual Machine

The complete and tested automation tool was hosted in a cloud Virtual private server with the following specifications:

Table 3 - Hosted on Cloud Server Features, Source: Author.

Component	Specification
Main Memory	4GB RAM
Processor	2 CPU Cores
Storage	48 GB SSD Storage
Network	40Gbps Network in , 1GB Network Out
Transfer capacity	2 TB

4.6.3 Development environment

The Automation tool was developed and implemented on an environment with the following specifications:

Table 4 - Automation tool Development Environment Features, Source: Author.

Component	Specification
Programming Language	PHP
Framework	Laravel web-based PHP framework
Database	SQL Server
Network	40Gbps Network in , 1GB Network Out
Cloud Operating System	Ubuntu 16 LTS
Deployment	IaaS Cloud Virtual Machine

Browser	Firefox, chromium
---------	-------------------

The Laravel framework was used for development of the automation tool. Laravel is an open-source web-based PHP framework with a wide diversity of features and applications. This framework was chosen because of its diversity of use by many programmers and its ease of adaptation to the cloud environment. The framework is open source and therefore its acquisition and future scalability would be conducted with the utmost ease.

CHAPTER FIVE

RESULTS

Primary and secondary data sources were used in the data collection stage of this research. Data collected in the form of filled questionnaires were coded in SPSS by use of variables in the form of scale, ordinal and nominal. Nominal variables used in qualitative research provide a basis for classification. They are useful variables for generating categories and frequencies of qualitative findings. Ordinal variables' main aim is in providing more information about a subject matter. Scale variables, on the other hand, give a measure of an extent or a degree of extensity of a researched phenomenon. Analysis of data was entirely conducted on SPSS software. SPSS is an acronym for Statistical Package for Social Sciences and is an efficient statistician tool used in data analysis. SPSS was chosen by its popularity in researching the disciplines of academia and business. SPSS has also been used in the past by many scholars and also benefits from continuous upgrades and features optimizations from its developer thus maintaining its relevance and edge in data analysis (Arkkelin, 2014).

The most relevant features of SPSS used in this research are its ability to obtain descriptive statistics and inference from collected data of this study. Data collected in this study was in the form of filled questionnaires from a sample size of [twenty-five Organizations](#) who had undertaken an IaaS migration process at past. The intention of the data analysis of this study was in summarizing the respondents' characteristics that represented the most accurate perspective of the population of this study. This was later followed by drawing an inference from the summarized sampled population responses. The inference was drawn from the analysis of questionnaires collected during data collection. This inference was sourced through a presentation of findings in the form of frequency tables, measures of central tendencies and qualitative bar graphs. The crucial tasks in conducting an IaaS actual migration were then discussed. The necessary skills and team members were identified and the security requirements required in performing a complete IaaS migration identified. The below sections elaborate and present these findings in detail.

5.1. Primary Data Findings

The questionnaire shown in Appendix 5 was used to gather primary data. The Questionnaire was distributed through Survey Monkey, a software tool used to submit and collect responses from users in a distributed computing environment. By use of Survey monkey online tool. The

questionnaire was quickly distributed and responses received within shorter times as would have been if the questionnaire had been distributed through physical means.

5.1.1 Demographic information

Primary Data collection was conducted on a sample population of twenty-five respondents. This was as a result of purposive sampling that required identification of respondents who were knowledgeable and willing to give information on this study area. A total of twenty-five responses were initially sent via email Links to the sampled population. However, a total of twenty-one filled questionnaires were submitted back. This represented an 84 percent response rate and was satisfactory for this study. Among the received responses, there were twenty completely filled questionnaires and one questionnaire received had one question that did not have a response. This was achieved within the stipulated period and realized a response rate of 88.00 percent. Therefore, a total of twenty-two filled questionnaires were received with one of them having been incomplete. Complete questionnaires were used in the data analysis phase. A total of twenty-one were therefore usable for research analysis.

5.1.2 Experience in conducting an IaaS migration process

Purposive sampling requires the selection of respondents who are knowledgeable and experienced in a study area. For this research, these respondents were sourced on the basis of experience and willingness to give the information requested by this study. Knowledge as an aspect of measure of expertise in a study area was invoked in generating this question. The respondents were asked to indicate the number of years they had worked in IaaS cloud migration and IaaS cloud administration. This question's intention sought to ensure that the respondents in this question were dependable, had a well understanding and knowledge of the subject matter. A rating scale was used to capture the responses. The findings are summarized in the table below:

Table 5 - IaaS Migration Experience, Source: Author.

		Frequency	Percent	Valid Percent
Valid	1 Year	4	19.0	19.0
	2-3 Years	9	42.9	42.9
	4-6 Years	7	33.3	33.3
	6-10 Years	1	4.8	4.8
	Total	21	100.0	100.0

The data in Table 5 above was computed as follows:

Frequency= the number of respondents that submitted the specific range of years' experience.

Percent= A percentage of frequency range over the total number of respondents.

Valid Percent= a percentage of frequency over the total number of responses.

A total of twenty-one filled questionnaires were received. All respondents provided the feedback required for further analysis of this question. This is, therefore, a 100 percent response rate to this question. We conclude with 100.0 percent confidence that all respondents had prior experience in migrating services to the IaaS cloud. Their responses were, therefore, valid for analysis in this study. A further investigation was conducted to draw an inference from the analyzed results displayed in Table 5 above. All the respondents had an IaaS migration experience ranging from 1 years to 10 years with a majority having attained an experience of over two years. The results in Table 5 above indicated that 19 percent of respondents had achieved over one years' experience in cloud migration, 42 percent had an experience ranging between two and three years', 33.3 percent had between four and six years' knowledge on the subject under study, and 4.8 percent had attained an experience ranging from six to ten years in IaaS cloud migration in Kenya. This was further analyzed through the generation of mean, median, mode, Standard deviation, Minimum and maximum years of experience. The results are displayed in Table 6 below:

Table 6 – IaaS Migration central tendencies, Source: Author.

N	Valid	21
	Missing	0
Mean		2.2381
Median		2.0000
Mode		2.00
Std. Deviation		.83095
Minimum		1.00
Maximum		4.00

The mean experience among all respondents analyzed was an experience of two years in migrating services to the IaaS cloud. The most experienced respondents had at least four years' experience in IaaS cloud migration. Table 5 and Table 6 analysis confirmed that all respondents had undertaken an IaaS migration at past and had experience in deploying IaaS clouds. We, therefore, conclude that the requirements of [purposive sampling](#) were met in the identification of the correct sample that represented the phenomenon of the larger population in this research.

5.1.3 Cloud providers of choice in IaaS migration

IaaS clouds are characterized by many providers who offer their clouds to adopters. The adopter has a preliminary choice of the IaaS provider to engage with and launch their systems to the provider's cloud. For this reason, it was important to find out the most common types of IaaS providers used by Kenyan SMEs while deploying their systems to the cloud. This was the main objective for this question. The findings from analysis to this question further aided scoping and customization of the output tool of this research and also ensured that [the automation output tool](#) developed, represented the best options for SMEs while configuring their IaaS cloud instances and Virtual Machines (VMs). The findings are summarized in the table below:

Table 7 – IaaS provider choices, Source: Author.

\$provider Frequencies

		Responses	
		N	Percent
\$provider^a	Digital Ocean Provider	4	10.8%
	GCloud	5	13.5%
	Sasahost	8	21.6%
	AWS	7	18.9%
	Safaricom Cloud	7	18.9%
	Azure	2	5.4%
	Linode	4	10.8%
Total		37	100.0%

A total of twenty-one questionnaires were received with twenty of them having given a feedback to this question. This was a 95.2 percent response rate to this question. We conclude with a 95.2 percent confidence that the IaaS cloud providers of choice are Sasahost with 21.6 percent, Safaricom Cloud with 18.9 percent, Amazon Web services with 18.9 percent, Google cloud (GCloud) with 13.5 percent, Linode with 10.8 percent, Digital Ocean with a 10.8 percent and Microsoft Azure(MSAzure) with 5.4 percent. The top three IaaS providers of choice are Sasahost, Amazon Web Services (AWS) and Safaricom Cloud. It was also noted that the leading two providers of choice had physical offices within Kenya where this study was conducted. From the data presented in Table 7 above, it was observed that the total responses received for the question which exceeded the number of respondents sampled. Further analysis was drawn as represented in the table below with the aim of understanding the phenomenon that was being portrayed.

Table 8– IaaS Provider responses variance analysis, Source: Author.

	Responses Percentage	Percent Of Cases	Variation Index
Digital Ocean Provider	10.8	20.0	1.9
Gcloud	13.5	25.0	1.9
Sasahost	21.6	40.0	1.9
AWS	18.9	35.0	1.9
Safaricom Cloud	18.9	35.0	1.9
Azure	5.4	10.0	1.9
Linode	10.8	20.0	1.9
Total	100	185.0	1.9

The data in Table 8 above sought to determine the variance between the total responses and the number of cases. The Variance index was computed as follows:

Variance index= A factor that indicates the difference between two figures

Responses percentage= the percentage of the responses per each provider

Percent of cases= the percentage of cases realized per the number of respondents to each provider

Variance index= Percentage of cases/Responses Percentage

According to the data presented in Table 8 above, it was observed that the number of cases exceeded the number of respondents to this specific question. Through the generation of the variance index, it was inferred that a number of respondents had acquired experience with more than one IaaS provider.

5.1.4 IaaS Virtual machine (VM) instances accessed

IaaS providers' cloud relay different types of virtual machines for purchase and use by an adopter while deploying systems to the IaaS cloud. This is information relevant to this study as it best represents the most preferred virtual machine instances while deploying systems to the IaaS cloud. The inference drawn from analysis of responses provided for this question was later used in

designing components of [the automation tool](#) which was the output of this study. To find out the types of IaaS virtual instances used to host services on the IaaS cloud, respondents were asked to list the different types of IaaS cloud VM instances they had used. The findings are summarized in the Table 9 below:

Table 9 – IaaS Virtual Machines Instances Used, Source: Author.

		Responses	
		N	Percent
\$VMinstance^a	Shared Hosting	13	28.3%
	VPS Servers	13	28.3%
	Dedicated Servers	13	28.3%
	Offsite Data Centre(DC)	7	15.2%
Total		46	100.0%

All respondents provided feedback to this question. We, therefore, conclude with a 100 percent confidence that the most preferred types of VMs in Kenya have shared hosting, Virtual private servers(VPS) and Dedicated servers at 13 percent each. Offsite Data Centre virtual machines follow with 7 percent likelihood of use. The number of cases submitted in Table 9 above exceeded the number of respondents sampled. Additional analysis was conducted to determine and draw an inference of the mismatch between number of respondents sampled and the number of case obtained. The findings are displayed in Table 10 below:

Table 10 – IaaS Virtual Machines responses variance analysis, Source: Author.

	Responses Percentage	Percent Of Cases	Variation Index
Shared Hosting	28.3	61.9	2.2
VPS Servers	28.3	61.9	2.2
Dedicated Servers	28.3	61.9	2.2
Offsite Datacentre(DC)	15.2	33.3	2.2
Total	100	219.0	2.2

From the data presented in Table 10 above, we conclude that most the respondents had used more than one type of IaaS VMs at an index of 2.2. Therefore, we infer that the adopter may use different types of virtual machines while migrating the different system to the IaaS cloud.

5.1.5 Essential IT technical skill sets in IaaS migration

To identify the critical technical team attributes in Rehosting systems on an IaaS cloud, the respondents were asked to indicate the necessary skill sets required for a successful and complete IaaS service migration. This question responses were meant to provide an answer to [the research objective 3](#). The findings are summarized in the table below:

Table 11 – Technical skills in IaaS actual migration, Source: Author.

		Responses	
		N	Percent
\$skillset^a	Systems Development	19	19.6%
	Cyber Security	15	15.5%
	Network Administration	19	19.6%
	Cloud Infrastructure Administration	16	16.5%
	IT Support	8	8.2%
	Business Development	3	3.1%
	Customer Service	1	1.0%
	Database Administration	16	16.5%
Total	97	100.0%	

All respondents provided answers to this question as expected. This represents a 100 percent of the total response rate. We therefore conclude that the essential skill sets that collaborate in effecting a successful and complete migration of services to the IaaS cloud are Systems development skills at 19.6 percent, Cyber Security skills at 15.5 percent, Network administration skills at 19.6 percent, Cloud infrastructure skills at 16.5 percent, IT support skills at 8.2 percent, Business development at 3.1 percent, IT customer service skills at 1.0 percent and Database administration skills at 16.5 percent. However, the most prominent skills are Systems Development skills and Network administration skills with a 19.6percent index followed by Cloud

infrastructure administration skills and Cybersecurity skills at 16.5 percent and 15.5 percent respectively. The pie chart below further elaborates this aspect:

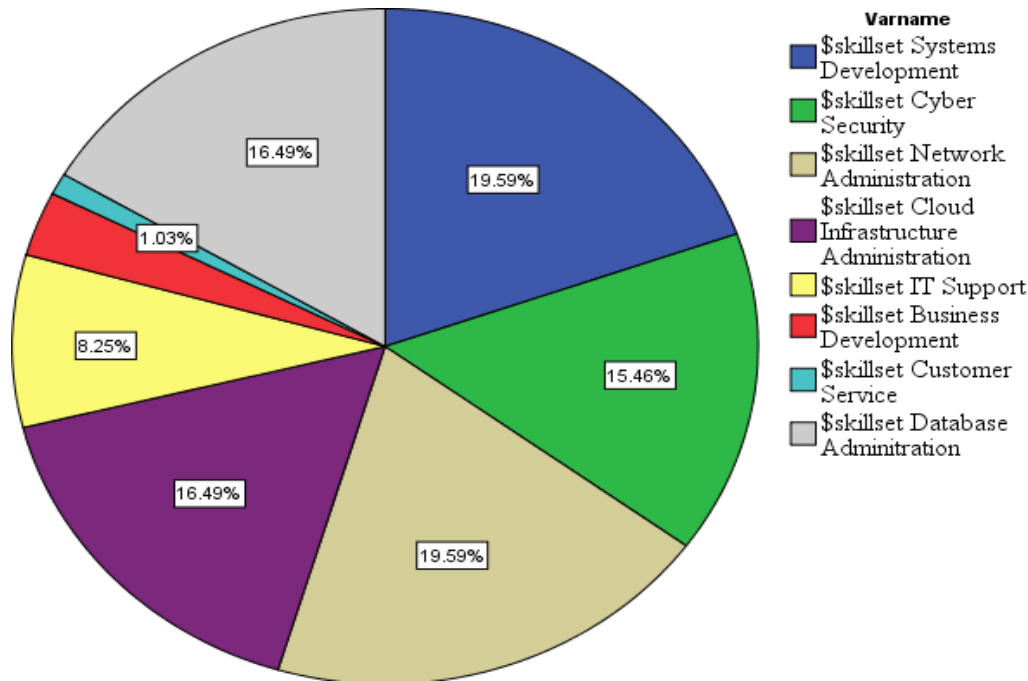


Figure 20 – Technical Skills distribution in IaaS migration

We conclude that there are four most essential technical skillsets required in effecting a complete IaaS service migration to the cloud. These are the skillsets that acquired at least an 8.25 percent preference. These are Network administration with 19.59 percent, Systems Development with 19.59 percent, Cloud infrastructure administration with 16.49 percent and Cybersecurity skills with 15.46 percent. For this reason, SMEs' should enhance their technical capacity in these major areas to ensure a complete and secure migration to the IaaS cloud.

5.1.6 Common Tasks and steps undertaken in actual service-migration to IaaS cloud

To identify the common key processes undertaken during Rehosting of systems from on-premise to the IaaS cloud, respondents were asked to indicate the tasks and steps they previously used in migrating services to the IaaS cloud. The respondents were required to fill in all the key stages they used in hosting systems to the IaaS cloud. This data was then analyzed using SPSS to identify the mode in the respective steps. The mode calculation was essential to identify the majority of

respondents who indicated that a particular activity was undertaken in a specific stage during the IaaS actual migration. The findings are summarized in the table 12 below:

Table 12 – Tasks and Steps in IaaS migration, Source: Author.

		Migration process:gain access to Virtual machine	deploy Operating system	Install App server eg apache	Patch Operating system and app server	Upload system files to cloud	Implement other security policies	configure cloud DNS	Test system components	Declare migration complete
N	Valid	21	21	21	21	21	21	21	21	21
	Missing	0	0	0	0	0	0	0	0	0
	Mean	1.0000	2.0476	3.0476	5.1905	4.8571	5.8571	7.3333	7.7143	8.6667
	Median	1.0000	2.0000	3.0000	4.0000	5.0000	6.0000	7.0000	8.0000	9.0000
	Mode	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00

Table 12 above indicates that there are nine key stages in an IaaS cloud which are executed procedurally. The nine key stages and activities during an IaaS migration are presented in Table 13:

Table 13: Stages in IaaS migration, Source: Author.

Precedence	Stage
Stage1	Gain Access to Virtual machine
Stage2	Deploy operating system
Stage3	Install App server
Stage4	Patch Operating System and App server
Stage5	Upload system files to cloud
Stage6	Implement security policies
Stage7	Configure DNS management
Stage 8	Test system components
Stage 9	Declare migration complete

Table 13 above indicates that an actual IaaS migration begins with access of credentials required to login to the IaaS instance on which applications are hosted. This is followed by deployment of a Cloud operating system which manages the cloud environment on which the hosted systems operate in. The third stage is deployment of an App server which provides the application environment required to host systems on the cloud. After this is done the Operating system and App server are hardened to prevent unauthorised access, during and after the following migration stages. Applications are then uploaded and configured on the IaaS cloud. The next stage that follows involves security policies implementations to further secure the hosted applications before their functionality testing begins. Testing of components involves a series of activities that ensure that all hosted components are working as required after their configuration on the IaaS cloud. Any errors and software bugs are then rectified during the testing of system components stage. This stage is continuous until all errors are fixed and their correct functionalities confirmed by the system development and the business team. Upon completion of all stages required, the Project manager declares the closure of the IaaS migration project.

5.1.7 IaaS Cloud security during migration

To identify the key security policies required in conducting a secure IaaS cloud migration process, respondents were asked to indicate all the security enforcements they effected on IaaS clouds in securing their hosted systems. The findings are presented in the table 14 below:

Table 14 – Security in IaaS migration, Source: Author.

		Responses	
		N	Percent
\$Sec_ ^a	ACLs	10	14.9%
	VPN	13	19.4%
	Access control (Username and Passwords)	14	20.9%
	Public Private Key cryptography	13	19.4%
	Hashes	4	6.0%
	SSL	11	16.4%
	RBAC	2	3.0%
	Total	67	100.0%

We conclude that the security implementations used in securing an IaaS cloud include Access Control lists(ACLs) with 14.9 percent, Virtual Private Networks(VPNs) with 19.4 percent, Username and Passwords access control with 20.9 percent, Public-Private Key cryptography with 19.4 percent, Secure Socket Layer(SSL) with 16.4 percent and Role-based access controls(RBAC) with 3 percent preferences. The figure 2 below further illustrates this:

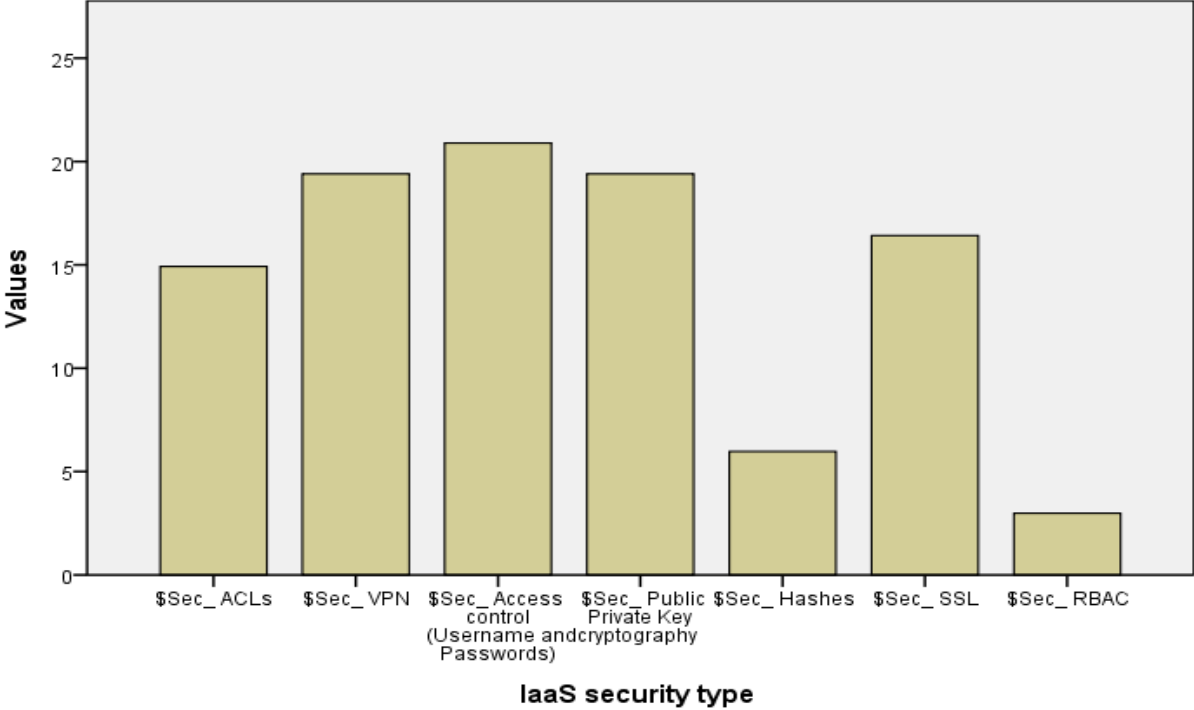


Figure 21 – presentation of IaaS security types during IaaS migration, Source: Author.

The Figure 21 above indicate that most IaaS clouds implement SSL, VPNs and Public-private key cryptographic algorithms. These security implementations could be adopted into new IaaS migrations to enhance the security of the process and applications hosted on the IaaS clouds.

5.2. Secondary Data Findings

Secondary data was sourced with the main aim of identifying configurations in the live IaaS cloud environment. This information was sourced from Roamtech solutions Limited Kenya IaaS cloud which hosts over 10 systems on their cloud. The main systems of focus were the IVR voice service used by the call center and the messaging server used for provision of SMS services such as USSD, shortcode and Bulk SMS. Secondary data was collected through interview with the head of IT infrastructure, Head development and Head of Networks. Additional information was sourced from ICT archival documents and review of configurations in the live servers' environment as presented in the sections below.

5.2.1 Network Setup

The Network is set up for access both from the company intranet and public access. The company intranet comprises of Cisco 2900 series router and distribution switches for the physical topology. The logical topology comprises of Vlans propagated within different departments for data and voice services access. Voice access contains LAN voice services and public customer service interactive voice response (IVR) for external public phone network call routing. The production network is a point-to-point link between the company intranet and remote data centre. The logical connection is a WAN-Link across two Internet Service Providers secured via VPNs. The Internal connection of the production network implements VLANs that distinguish between services hosted in the remote data centre. Data services are supplied via three redundant ISP fibre links by Jamii Telkom Limited, Liquid Telkom and Telkom Kenya.

5.2.2 Server Setup

The infrastructure contains multiple servers hosted at the company Internal server room and others hosted on the remote IaaS cloud. The remote IaaS cloud utilizes Ubuntu and Centos Operating systems. The App server installed is Apache and Ginnx. Critical servers host single computing systems while other servers co-host multiple computing systems via different instances. The IaaS provider in use is Gcloud, and multiple instances are deployed for each computing system hosted. Access to servers' management API is restricted to company technical department staff and is only accessed from the company's intranet. However, other customer service systems are accessed by the public with the backend access restricted to the customer service officers. The Interactive voice

response(IVR) system is only accessed by the customer service departments and hosted on the remote IaaS cloud.

5.2.3 Stages in IaaS migration

The process of migration in Roamtech Limited is initiated by approval to commission a service or product to be hosted on the company's production cloud. The essential teams comprised of system developers, networks, infrastructure team and the IT manager agree on a date to execute the migration from the Internal development server to the company's cloud. Once this is done, the accounts department procures any needed resource such as server space or additional network racks and hands over to the networks and infrastructure team. The network and infrastructure team upon receipt of all necessary physical resources and the GCloud login credentials provision the instances on the Gcloud on which the systems will be migrated to. Software in use includes PUTTY and Gcloud web portals. The next step is configuration of SSH and Telnet services to the deployed Gcloud instances. The Operating system chosen is then deployed, updated and VIM editor and appserver installation follows immediately after.

The Appservers of choice are Nginx and Apache. However, Apache is preferred to run most applications on the cloud since majority team members have a prior experience of its use. Nginx servers are used for load balancing as they are light in resource consumption and have faster execution speeds. For Roamtech solutions limited, Nginx servers are used as servers to other apache clients. The Application essential environments such as the framework, and the database are then installed on the cloud server. Preliminary testing is then conducted to ensure that the cloud is set up correctly before initializing the application transfer process. Application transfer process is effected by the developers and involves pushing the system files to the cloud. In other scenarios, the application may be pre-hosted in Git hub and pulled from the specific directories during the application transfer process. Once the application transfer process completes, DNS management is configured by the Infrastructure team and any necessary VPNs are created to secure its access. This is followed by the implementation of needed security policies according to the company policy. The Last step is testing of the application functionality and effecting necessary changes of its optimization to effectively render its services while on cloud. Once this is done, the migration process is declared complete.

5.2.4 Security in IaaS migration

Once this is done, the migration process is declared complete. Security of the cloud-hosted applications is a key concern in Roamtech solutions Limited. Majority of the tasks involving security implementations are conducted by the infrastructure team since there is no designated cyber security staff. Security starts after provisioning the virtual instances. The main type of security in this stage is Identity access management which provides access control to staff members who use the cloud. Implementations here include usernames and passwords, and access control lists.

Other security measures involve analysis of server authentication logs upon a complete IaaS migration. The Logs analysis involve identification of bots and other IP-addresses constantly seeking access to the IaaS servers. Any malicious entries are blocked via access control list route firewall. Roamtech solutions limited's IT department security minimums require configuration of SSL on all cloud servers. For this reason, all cloud servers have installed SSL certificates for all their operations. The production environment also has several servers each with different levels of security. For instance, a broker server is installed and negotiates services between other servers that render services to it. This is a security measure that restrict access to all servers at a single instance. This also increases the robustness of the company cloud further increasing the learning curve duration for potential attackers.

5.3. Discussion

This section observes the findings already presented in sections 5.1 and 5.2. The entire discussion in this section is based on the preliminary objectives for which this study was conducted. Section 5.3.1 summarises the discussion around the choice of the IaaS provider on which systems are configured on. Section 5.3.2 continues to discuss the hosting options and considerations made by adopters after choosing the IaaS provider. Section 5.3.3 then discusses in detail the process of IaaS migration with a focus on the common tasks identified from both the primary data collection and secondary data collection sections in this study. This section further concludes by discussing the inference used to generate the model and stages of IaaS migration which was presented and tested by the output tool presented in Chapter 4.

5.3.1. IaaS Adopters choices of Cloud Providers

Majority of IaaS adopters in Kenya choose a cloud provider nearest to their geographical location due to more approachable technical support and increased trust. Provider trust was also identified as a crucial decision metric for IaaS adopter by Singh et al., (2014) through a study conducted in Europe. The study by Singh et al., (2014) identified that trust was a critical and a must consider metrics while choosing an IaaS, cloud provider. Underpinning this was the inference that the IaaS Cloud provider chosen has a secondary ownership of configured systems and hosted data thus adopters must have the confidence of proper handling of their data in the cloud. For the Kenyan case, the inference in this thesis was drawn from the antecedent that the top three cloud providers of choice identified in section 5.1.3 were Sasahost and Safaricom cloud then closely followed by Amazon. An inference is therefore drawn that the majority of already configured IaaS clouds in Kenya implement technologies supported and fostered by these cloud providers. These findings present an important knowledge pool for any SME that consider to configure its systems on an IaaS cloud. Therefore, SMEs who further adopt these IaaS providers stand to benefit from a broader IaaS migration pool of knowledge already existing in Kenya. In a case of misconfigurations, while undertaking the actual IaaS migration process on these IaaS clouds, the technical team in Kenyan SMEs would benefit from further support by professionals who had undertaken a similar migration project at past. Furthermore, a geographically approachable provider would mean that an SME would have increased confidence in choosing their IaaS cloud providers as this is an indicator of a faster and a more approachable technical support.

5.3.2. IaaS Hosting choices

The choice of the hosting options to launch systems on the IaaS cloud is a choice that the technical team involved in the process make before just before commissioning the IaaS migration process. This originates from the fact that the adopters share the cloud providers computing infrastructure and access virtual machines specific to their purchased IaaS cloud instances. Section 5.1.4 enlisted the hosting options offered by the different providers as shared hosting, Virtual private serves, dedicated servers and remoted data centers.

Shared hosting provides a more economic option to adopters where all adopters systems reside on a single webserver offered by an IaaS provider. However, each adopter's system resides in own

partition which separates it from the others. A Virtual Private Server(VPS) presents a virtual machine relayed as an instance. A VPS has its own operating system specific only to the adopter. A dedicated server offers an entire virtual server for use by the adopter. Remote data center offers virtualized grid computers with conventional high performances to the adopters (Sen, 2017). Section 5.1.4 of this research identified a balanced preference between the three main IaaS cloud virtual instances of shared hosting, VPS servers and dedicated servers followed by offsite datacentre. Therefore, for any Organisations preparing to launch systems to the cloud the need to acquire knowledge on implementation of technologies on these three IaaS virtual instances is crucial.

5.3.3. Collaboration of Technical skillsets during actual IaaS Migration

Technical team collaboration according to Yousif (2016) was critical in undertaking a complete IaaS migration. Objective 3 of this study sought to identify the technical teams needed to conduct a successful IaaS actual migration process. The technical skillsets identified in section 5.1.5 were Network Administration, Cloud infrastructure administration, Systems development, Cyber Security skills, Database administration, and Business development. Inference is drawn that these are the critical skills that collaborate to effect a complete IaaS migration project.

Network administration is a skill that entails keeping the operations of a company's network, its connected computing devices, and configured systems smooth and running. An ideal job description of network administrators includes the key duties of ensuring that network devices and systems are installed, maintained, network services are monitored to improve their performance and occasionally repairs and fixes problems that may arise in their network environments. A cloud infrastructure administrator is a professional with the combined knowledge of network administration and virtualized environments.

The cloud infrastructure administrator is the technical staff that works closely with the operational leads and other cloud administration staff to ensure that cloud systems are well configured and meets their intended business needs. Cyber security professionals are responsible for design, implementation and administration of firewalls, intrusion detection systems and other information security safeguards that protect the computing environment. Database administrators ensure that the information stored on databases enforce integrity and are secure from unauthorised access from

exploited database vulnerabilities. System developers are responsible for development and implementation of computer software used in businesses and organisations. Business development professionals, on the other hand, use the developed systems and business software to fulfill customers' needs and in pursuit of new clients.

Technical skills collaboration during cloud migration is a phenomenon also upheld by Roamtech solutions Limited as elaborated by secondary data findings presented in section 5.2.3 of this research. The migration process findings at Roamtech Solutions limited was effected through the collaboration of various skillsets of system developers, network and infrastructure administrators and the IT manager who supervised the migration process. However, different stages of migration are effected by different technical skillsets.

5.3.3. IaaS Migration Process

The migration process begins by gaining access to the IaaS instance on which the systems are configured on. This is followed by a next stage that involves selection and deployment of an operating system of choice as described in section 5.1.6. The adopter then proceeds to install the App server which is the environment in which the deployed systems operate from. Section 5.2.3 further indicates that the same processes were undertaken at Roamtech solutions limited. Apache and Nginx are the leading application environments most preferred in Kenya. Secondary findings identified that Apache was leading as was the most common environment in which the systems and applications were built on. This is then followed by implementation of preliminary security implementations meant to secure the operating system and the app server by the cyber security professionals.

The secondary data findings indicated that these security policies included Identity access management, patching the operating system and the app server installed in the previous stages. These security implementations serve the purpose of securing the cloud virtual machine from malicious attacks during the applications hosting process. Applications are then launched to the cloud by the system developers. Completion of this stage marks the beginning of a further security process geared towards the hosted applications and data as a whole. Security implementations here include VPNs, ACLS, and common application attacks prevention policies. After this is done, the application is taken through several tasks of testing that ensure its completeness in adaptation to

the cloud. The results of the secondary data findings in Section 5.2.3 indicated that all the application components are tested by the system developers and the business developers until both teams are satisfied with their completeness in configuration and functionalities. The project manager then marks the migration process as complete upon successful completion of these stages.

Section 5.1.6 breaks the process of IaaS migration into a series of 9 stages from the finding in Sections 5.2.3 and 5.1.7. An organisation in that undertakes these steps procedurally stands an advantage of realisation of a complete IaaS migration. Through collaboration and execution of stages in migration in a series of key stages, Roamtech solutions Limited boasts of over ten computing systems already configured and securely accessed on the IaaS cloud. These stages and tasks were additionally used to generate the functional requirements of the automation tool described in chapter 4 of this study.

5.4. Chapter Summary

This chapter presented the results and analysis and discussions of data collected in the data collection stages of Chapter 3 of this thesis. The discussions in this chapter were mainly focussed on the main concepts under research which included the process of conducting an actual IaaS migration, the IaaS cloud choices and instances chosen and the security policies implemented in securing the IaaS cloud. The process of migration stages was examined to identify similarities through the experience of the sampled population in Chapter 3. The common steps were then classified into definite migration stages which required to be executed sequentially. Under the Contest of Kenya SMEs, the migration stages and process were then used to develop the automation tool presented in Chapter 4 of this thesis. The next chapter concludes the study and terminates after making recommendations for future studies.

CHAPTER SIX

CONCLUSION

6.1. Introduction

In this study, the actual IaaS migration was presented as a series of stages with tasks that needed execution in a sequential manner. This study generates and automated a model through which SME's in Kenya could use to acquire knowledge on the execution, precedence, and experience of migrating system components to the IaaS cloud. We also looked at the critical teams that collaborated in migrating systems to the IaaS cloud and incorporated their roles and responsibilities in the automation tool derived in this research. In the output tool of this research, technical skillsets required during an IaaS migration collaborate in executing the different stages and tasks during the IaaS migration. We also looked at the contribution of cyber security professionals and their participation in the IaaS migration process. The execution of stages and tasks was presented as a sequential process comprised of task and precedence metrics that ensured synergy and traceability of the process. The role of the project manager as the overall supervisor and owner of the project was then included in the automation tool and an ability to generate a report upon completion of a migration project.

6.2. Research Objectives Achievement

Taking everything into consideration, this study has realised all its intended objectives with the following justifications:

a) **Objective 1-** To identify common key processes undertaken when migrating systems from on-premise to IaaS cloud.

In the literature review presented in Chapter 2, we reviewed the existing body of knowledge and identified the gaps yet to be filled by past scholars on the topic of IaaS actual migration. This review is well elaborated in sections 2.6 and 2.7 of this thesis. We identified that while past researches majorly focused on the development of IaaS migration models, not much had been done in the actual migration of systems to the IaaS cloud. Yousif (2016) had discussed the technical skills gap that SMEs struggle with whenever they are deploying systems to the IaaS cloud. The actual IaaS migration was said to be a complex process with many security risks and tasks that needed to be put into account to achieve a complete migration. Despite the cost benefits realised

from running the IT infrastructure from the cloud, SMEs were hesitant to adopt the IaaS cloud majorly due to technical skills gap (Adricopulous,2013). Moving to the IaaS cloud attracted huge costs to SMEs due to over-reliance on migration expertise for consultancy and help in deployment of systems to the cloud (Nicholas,2013). Wanjiku (2014) had further noted that most ICT officers in Kenya had a good understanding of the operations of Network and databases which were essential skills that were not effectively applied while setting up private clouds. This work by Wanjiku (2014) identified a gap in the skills and knowledge of deploying systems to the IaaS public clouds. To address this skills gap challenge, Yousif(2016) identified the huge opportunity for SMEs to build migration expertise within their technical skillsets over time that would help instill essential skills required for a complete IaaS migration. Yousif (2016) further identified a need to ease the complexities of IaaS migrations by selectively studying organisations who had migrated systems before and identified patterns in the processes of their IaaS actual migration. This was the basis for development of this objective.

By performing the data collection exercise detailed in section 3.4, we identified a pattern and the similar tasks that past SMEs had effected when they hosted their systems to the cloud. This was then used to derive a sequence and stages of the IaaS actual migration process presented in section 5.1.6 of this study. The similar stages derived from the study of organisations selected for this research were identified as: gaining access to the IaaS cloud, deployment of operating system on the IaaS cloud, installation of App server, patching installed operating system, patching app server, uploading of systems files to the cloud, implementation of essential cloud security policies, configuration of DNS management and testing of systems components to ensure their completeness in functionalities on the new IaaS cloud. These stages were executed in a chronological order during an IaaS actual migration and were crucial in achieving a complete migration as presented in section 5.1.6 of this thesis. The secondary data findings further give in detail, the roles and responsibilities of team members who collaborate to effect the IaaS migration. When SMEs decide to host their systems on IaaS clouds and adopt the model automated in this research study, they stand to achieve the benefits of realisation of the technical skills collaboration which at the end result to a complete and successful migration project.

b) **Objective 2-** To identify key security policies required in conducting a secure IaaS cloud migration process

Having identified the crucial need of security on and during IaaS cloud migration in section 2.3 of the literature review, we sort out to identify the key cloud security policies implemented during an IaaS migration. We studied the security policies that were implemented by the research population. Realisation of this objective involved a case by case analysis of the security policies implementations in the sampled population who had undertaken an IaaS migration before. This is well elaborated in Section 5.1.7 of this thesis. The findings indicated that while most IaaS clouds implement Access control by means of authentication through username and passwords, other security policies implemented on the IaaS cloud included Virtual Private Networks(VPN), Public-Private Key cryptography, Secure Socket Layer(SSL), Hashes and Role Based Access Controls(RBAC). These provided the main answer to this research objective and were further used to develop the answer to objective 4 of this research.

c) **Objective 3-** To identify the critical team attributes needed to effect a complete IaaS migration. Providing an answer to this research objective was the most demanding in terms of time invested. The Literature review in section 2.6 had already identified past scholarly work that identified the need to adopt a team approach while conducting an IaaS migration. This is through the findings of a study conducted by Rosaldo (2013) that identified business development team, technical team, support team and project management team as critical teams to put into consideration during an IaaS migration. In this study, we sought to find out if this was the case in Kenya. The primary data findings in section 5.1.5 and secondary data findings of section 5.2 of this research were the most useful in realisation of this objective.

We identified that the most critical skillsets required to conduct a complete IaaS migration were network administration, systems development, cloud infrastructure administration, cyber security, database administration, IT support and Business development.

The next task was to find out the specific roles assigned to the identified skillsets during an IaaS migration. We then conducted the secondary data collection whose findings are detailed in section 5.2 of this thesis. We identified that Cloud and Network infrastructure administration was essential in Gaining access to the IaaS Cloud(Stage1), Deployment of operating system(stage2), Deployment of App Server (Stage 3) and configuration of DNS management (Stage 7) of the IaaS migration stages presented in section 5.1.6 of this paper. System development was crucial in performing upload of files to the cloud (Stage 5) and testing of system components (Stage 8).

Cyber security skills were invoked in patching operating system and App server (Stage 4) and implementation of security policies (Stage 6). Business development skills were necessary for testing of system components newly configured on the IaaS cloud in Stage 8 of the IaaS migration. These findings formulated the answer to the objective 3 and question 4 of this study.

d) **Objective 4-** To develop a secure IaaS migration model and an automation tool.

The main aim in conducting this objective was to come up with a tool that would automate the stages and tasks conducted during an IaaS migration. The literature review detailed in section 2.7 had outlined the critical role of automation tools in easing the complexities of the IaaS cloud. Automation tools in our literature review were portrayed as the go to solutions in demystification of the IaaS cloud as they simplify the execution of tasks on the cloud. Automation tools portrayed a strong appeal of use to cloud administrators due to their inbuilt features that simplify the complexities of the IaaS migration.

Zhang and Shang (2014) had developed an automation tool that eased the process of deploying an operating system on the IaaS cloud. The main gains of this tool was that its users were able to launch operating system on the cloud without the help migration experts. This was an information tool which had focussed on execution of a single stage in IaaS migration. Our work involved developing an automation tool that would encompass information useful while conducting the stages identified in Objective 2 of this research. The functionalities of the automation tool developed in this research were derived from the gains achieved having fulfilled the previous three objectives of this research. Therefore, the automation tool was meant to test the gains realised by the other previous three objectives of the study. The process of its development is well elaborated in Chapter 4 of this thesis.

This tool presented the migration stages as isolated tasks that were performed sequentially and with precedence enforced. For this reason, the completion of a stage of migration gave way to the start of a next stage. This is presented in section 4.4. The skillsets realised by objective 3 formed the roles in the automation tool. Permissions to execute specific stages were strictly granted as per the findings of objective 3 of this research. Therefore, specific skillsets in IaaS migration were granted selective permissions to execute specified IaaS migration stages. The tool is also availed

as an open source software available online and under request for any future researcher who may want to further explore on this research study's gains.

6.3. Limitations of The Study

Number of Samples Used

There are very many organisations that had conducted an IaaS migration before. This study selected twenty-five organisations only. Therefore, conclusions and inference drawn in this study cannot be considered as the perfect representation of every other organisation in Kenya.

Sampling and Data collection

This study used purposive sampling which used the opinion of those who had conducted an IaaS migration before. This study did not critique or probe the why the samples had used the process of migration. Data collection used questionnaires as the main tool in primary data collection. The responses were prone to subjectivity of the opinions portrayed by the respondents chosen.

Challenges in Available Resources

All finances used to conduct this study were self-sponsored and this was a limitation to the literature and number of respondents used in this research.

Lack of an on open source migration tool

During the entire duration of this research execution, there was no known open source automation tool available for referencing and benchmarking.

6.4. Future Research

The study detailed in this paper focused on development and automation of a model for IaaS migration that could be used by SMEs in Kenya whenever they launch their systems on the cloud. The output tool of this research was an automation tool with detailed information on IaaS migration to be used by SMEs whenever they conduct an actual migration. Therefore, to further utilise the gains achieved in this study, we make the following recommendations for future studies:

- Future studies to involve adapting other domain areas not included in this study or extend the domain within which this research falls in.

- To extend the functionalities of the automation tool of this research to include APIs with endpoints linking to the identified IaaS providers' cloud. This is because direct linkage to these providers' cloud from the tool proposed in this research would result to an improved user journey and result in better acceptance of this tool.
- Future researchers to test the automation tool proposed in this research in specific organisation to further track its relevance and completeness in automation of all stages and tasks during an IaaS migration.
- Future research to study in depth the cloud security implementations identified in this paper such as VPNs, ACLs, Public Private Key cryptography, SSL and RBAC through practical case studies of their implementation in selected organisations with an IaaS cloud already provisioned. This will help extend this research domain.
- Pro-test this research finding over time to maintain its relevance and optimise its output tool.

REFERENCES

1. Adam, I. and Musah, A. (2015). Small and Medium Enterprises (SMEs) in the Cloud in Developing Countries: A Synthesis of the Literature and Future Research Directions. *Journal of Management and Sustainability*, 5(1).
2. Amazon (2015). *A Practical Guide to Cloud Migration Migrating Services to AWS*. [online] Available at: <https://d0.awsstatic.com/whitepapers/the-path-to-the-cloud-dec2015.pdf> [Accessed 8 May 2017].
3. Amorim, G. (2014). The Importance of SOA to Cloud Computing. [online] *Service Technology Magazine*. Available at: <http://www.servicetechmag.com/I87/1214-3> [Accessed 5 May 2017].
4. Andrikopoulos, V., Binz, T., Leymann, F. and Strauch, S. (2012). How to adapt applications for the Cloud environment. *Computing*, 95(6), pp.493-535.
5. Anon, (2017). [online] Available at: http://careers.ieee.org/virtual_career_fair/pdf/Microsoft_Cloud_Whitepaper.pdf [Accessed 2 Aug. 2017].
6. Arkkelin, D. (2014). *Using SPSS to Understand Research and Data Analysis*. Valparaiso University: ValpoScholar Psychology Curricular Materials.
7. Astri, L. (2015) "A Study Literature Of Critical Success Factors Of Cloud Computing In Organizations". *Procedia Computer Science* 59 : 188-194. Web.
8. Austin, Z. and Sutton, J. (2014). *Qualitative Research: Getting Started*. *The Canadian Journal of Hospital Pharmacy*, 67(6).
9. Bhardwaj, S., Jain, S. and Jain, L. (2010). CLOUD COMPUTING: A STUDY OF INFRASTRUCTURE AS A SERVICE (IAAS). *International Journal of Engineering and Information Technology*, 2(1), pp.60-63.
10. Callanan, S., O'Shea, D. and O'Regan, E. (2016). Automated Environment Migration to the Cloud. *2016 27th Irish Signals and Systems Conference (ISSC)*.
11. Candel Haug, K., Kretschmer, T. and Strobel, T. (2016). Cloud adaptiveness within industry sectors – Measurement and observations. *Telecommunications Policy*, 40(4), pp.291-306.

12. Cio.co.ke. (2016). SEACOM helps Kenyan organisations accelerate their migration to the cloud - CIO East Africa. [online] Available at: <http://www.cio.co.ke/news/top-stories/seacom-helps-kenyan-organisations-accelerate-their-migration-to-the-cloud> [Accessed 6 May 2017].
13. Columbus, L. (2015). *55% of Enterprises Predict Cloud Computing Will Enable New Business Models In Three Years*. [online] Forbes.com. Available at: <https://www.forbes.com/sites/louiscolombus/2015/06/08/55-of-enterprises-predict-cloud-computing-will-enable-new-business-models-in-three-years/#22bfa4c17582> [Accessed 8 May 2017].
14. Columbus,L (2015). Roundup Of Small & Medium Business Cloud Computing Forecasts And Market Estimates. [online] Available at: <https://www.forbes.com/sites/louiscolombus/2013/07/30/roundup-of-small-medium-business-cloud-computing-forecasts-and-market-estimates-2013/#325312397efd>.
15. Field, A., Miles, J. and Field, Z. (2014). *Discovering statistics using R*. London: Sage, p.925.
16. Gupta, P., Seetharaman, A., & Raj, J. R. 2014. The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, 33(5), 861-874.
17. J, P., Pawar, A. and V, N. (2017). A REVIEW OF EXISTING CLOUD AUTOMATION TOOLS. *Asian Journal of Pharmaceutical and Clinical Research*, 10(13), p.471.
18. Jackson, T. (2014). SA, Kenya cloud revenues to more than double by 2018. [online] BiztechAfrica. Available at: <http://www.biztechafrika.com/article/sa-kenya-cloud-revenues-more-double-2018/8762/> [Accessed 6 May 2017].
19. Jamshidi, P., Ahmad, A. and Pahl, C., 2013. Cloud migration research: a systematic review. *IEEE Transactions on Cloud Computing*, 1(2), pp.142-157. Khajeh-Hosseini, A., Greenwood, D. and Sommerville, I., 2010, July. Cloud migration: A case study of migrating an enterprise it system to Iaas. In *Cloud Computing (CLOUD)*, 2010 IEEE 3rd International Conference on (pp. 450-457). IEEE.
20. Khan, N. and Al-Yasiri, A. (2015). Framework for Cloud Computing Adoption: A Roadmap for Smes to Cloud Migration. *International Journal on Cloud Computing: Services and Architecture*, 5(5/6), pp.01-15.

21. Kofod-Petersen, A. (2014). How to do a Structured Literature Review in computer science. *semanticscholar*, 0.2.
22. Lewis, G., Litoiu, M. and Ionita, A. (2013). Migrating legacy applications: 1st ed. Hershey, Pa.: IGI Global (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA).
23. Mansouri, Y., Nadjaran Toosi, A. and Buyya, R. (2017). Cost Optimization for Dynamic Replication and Migration of Data in Cloud Data Centers. *IEEE Transactions on Cloud Computing*, pp.1-1. Raines, G. (2009). Cloud Computing and Service-Oriented Architecture (SOA). [online] The MITRE Corporation. Available at: https://www.mitre.org/sites/default/files/pdf/09_0743.pdf [Accessed 5 May 2017].
24. Marquez, L., G. Rosado, D., Mouratidis, H. and Fernandez Medina, E. (2016). Design Activity in the Process of Migrating Security Features to Cloud. *IEEE Latin America Transactions*, 14(6), pp.2846-2852.
25. Mazin Yousif.(2016). Migrating Applications to the Cloud. 1st ed. IEEE:
26. Merryman, J. (2015). Addressing Cloud Migration Complexity. [online] Glasshouse.io. Available at: http://glasshouse.io/addressing_cloud_migration_complexity_88 [Accessed 8 May 2017].
27. Monika, G. and Kalpana, Y. (2016). Data Security is the Major Issue in Cloud Computing - A Review. *Indian Journal of Science and Technology*, 9(43).
28. Nicolas ,N and Xiaodong. (2015). Cloud Migration for SMEs in a Service Oriented Approach. 1st ed. [ebook] Available at: <http://www.ccsenet.org/journal/index.php/jms/article/viewFile/43653/24671> [Accessed 22 May 2017].
29. Oun, M. and Bach, C. (2014). Qualitative Research Method Summary. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)* ISSN: 3159-0040, Vol. 1(Issue 5), pp.252-257.
30. Pahl C., Xiong H., Walshe R. (2013) A Comparison of On-Premise to Cloud Migration Approaches. In: Lau KK., Lamersdorf W., Pimentel E. (eds) *Service-Oriented and Cloud Computing. ESOC 2013. Lecture Notes in Computer Science*, vol 8135. Springer, Berlin, Heidelberg
31. Palinkas, L., Horwitz, S., Green, C., Wisdom, J., Duan, N. and Hoagwood, K. (2013). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method

- Implementation Research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), pp.533-544.
32. Rouse, M. (2013). What is Infrastructure as a Service (IaaS)?. [online] SearchCloudComputing. Available at: <http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS> [Accessed 8 May 2017].
 33. Sen, J. (2017). Security and Privacy Issues in Cloud Computing. Cloud Technology, pp.1585-1630.
 34. Singh, J., Bacon, J., Crowcroft, J., Madhavapeddy, A., Pasquier, T., Hon, K. and Millard, C. (2014). Regional clouds: technical considerations. Technical Report. [online] Cambridge CB3 0FD: University Of Cambridge. Available at: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-863.pdf> [Accessed 27 May 2018].
 35. Srirama, Satish & Ivanistsev, Vladislav & Jakovits, Pelle & Willmore, Chris. (2013). Direct migration of scientific computing experiments to the cloud. Proceedings of the 2013 International Conference on High Performance Computing and Simulation, HPCS 2013. 27-34. 10.1109/HPCSim.2013.6641389.
 36. Stallings, W. (2016). Network Security Essentials. Harlow, United Kingdom: Pearson Education Limited.
 37. Tavana, M. and Puranam, K. (2014). *Handbook of research on organizational transformations through big data analytics*. La Salle University, USA, pp.107-108.
 38. Tutunea, Mihaela Filofteia. "Smes' Perception On Cloud Computing Solutions". *Procedia Economics and Finance* 15 (2014): 514-521. Web.
 39. Wanjiku, R. (2017). Digital TV migration to provide business for Kenya's cloud provider | AfPIF 2017. [online] Internetsociety.org. Available at: <https://www.internetsociety.org/afpif/2017/en/news/digital-tv-migration-provide-business-kenya%E2%80%99s-cloud-provider> [Accessed 6 May 2017].
 40. Yousif, Mazin.(2016). "Migrating Applications To The Cloud". *IEEE Cloud Computing* 3.2 (2016): 4-5. Web.
 41. Yumoto, T., Matsuodani, T. and Tsuda, K. (2013). A Test Analysis Method for Black Box Testing Using AUT and Fault Knowledge. *Procedia Computer Science*, 22, pp.551-560.

42. Zhang, R., Shang, Y. and Zhang, S. (2014). An Automatic Deployment Mechanism on Cloud Computing Platform. *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, pp.511-518.

APPENDICES

Appendix 1: introduction letter to respondents

Dear Participant,

I invite you to participate in a research study entitled IAAS CLOUD MIGRATION MODEL FOR SMALL AND MEDIUM ENTERPRISES (SMES) IN KENYA. I am a graduate student enrolled in MSC. Distributed Computing Technology at The University of Nairobi and this survey is for the purpose of academic studies only. Because you or your IT-team previously conducted a systems hosting to a Virtual Private server (VPS), Dedicated server or any other Infrastructure-as-a-service provider servers, I am inviting you to participate in this research study by completing the attached surveys.

Your participation in this research project is completely voluntary. You may decline altogether, or leave blank any questions you don't wish to answer. There are no known risks to participation beyond those encountered in everyday life. Your responses will remain confidential and anonymous. Data from this research will be reported only as a collective combined total. No one other than the researcher will know your individual answers to this questionnaire.

If you agree to participate in this project, please answer the questions on the questionnaire as best you can. It should take approximately 5 Minutes to complete.

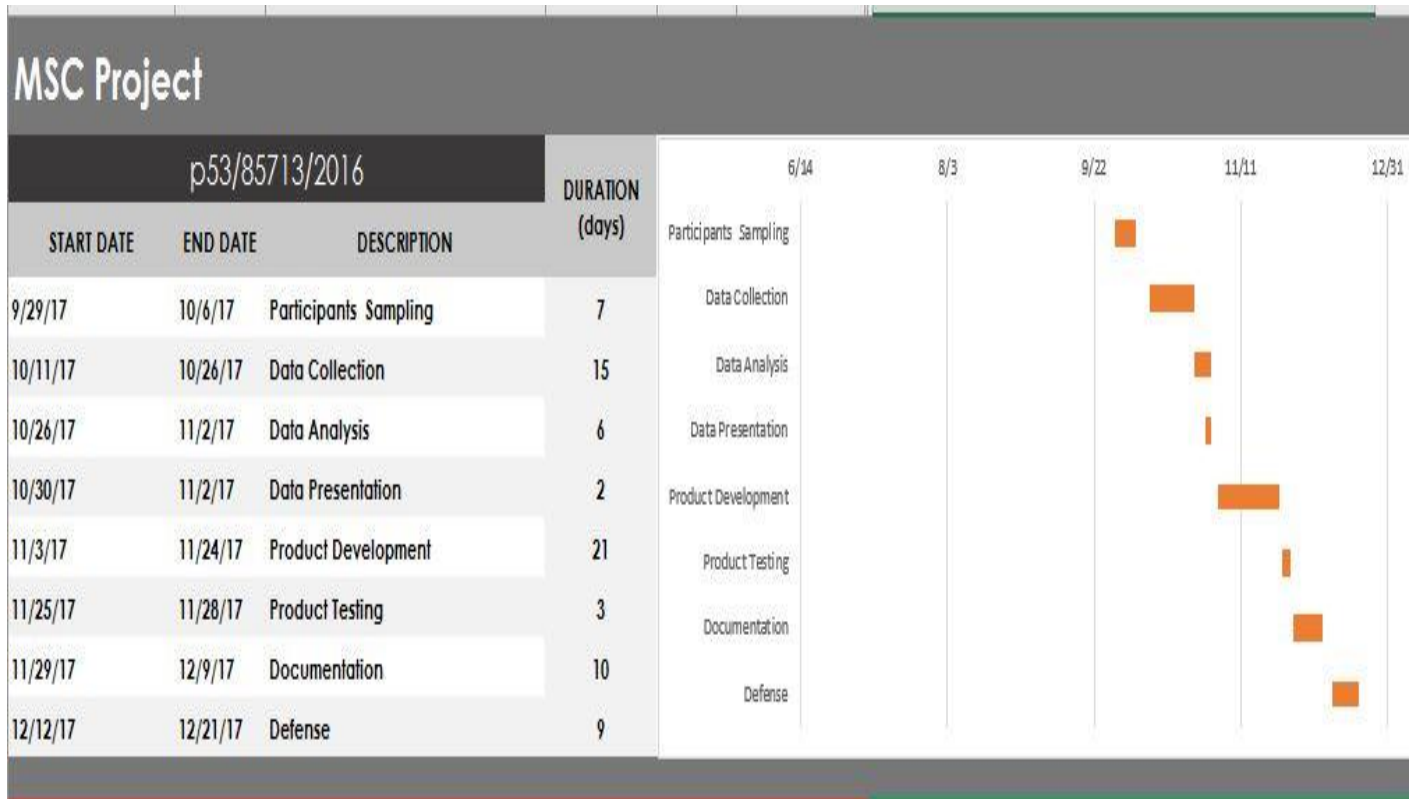
If you have any questions about this project, feel free to contact Kinaro Oreste - Researcher at orestekeikei@gmail.com

Thank you for your assistance in this important endeavour.

Sincerely yours,

KINARO ORESTE

Appendix 2: Research Schedule and Timeline



Appendix 3: Budget of Research

Task	Budget Allocation(Kshs)
IaaS server cost 6 months	45,000
Research Design and Analysis	24,000
Emergency Budget allowance	10,000
Domains and Equipment expenses	30,000
Total	109,000

Appendix 4: Technical Feasibility

Technical skill requirement	Availability	Competence Level
Cloud Server management	✓	Proficient
Linux administration	✓	Proficient
DNS technology	✓	Proficient
VM Virtualization	✓	Proficient
PHP development	✓	Intermediate
MySQL development	✓	Proficient

Appendix 5: Questionnaires or Interview scripts

University of Nairobi- Questionnaire on development and automation of a model for infrastructure service-migration to cloud

1. Name of Organisation

2. Designation of Respondent:

3. Duration worked in IT Industry (In Years):

- 1 Year
- 2-3 Years
- 4-6 Years
- 6-10 Years
- Above 10 Years

4. Duration worked in Cloud hosting or administration (In Years):

- 1 Year
- 2-3 Years
- 4-6 Years
- 6-10 Years
- Above 10 Years

. Which Cloud providers have you previously hosted your systems on?(Tick all that apply)

SasaHost

Digital Ocean

G cloud

AWS

Safaricom

Other (please specify)

6. Which cloud solutions have you worked with?

Shared Hosting

VPS Servers

Dedicated Servers

Offsite Data center Hosting

Other (please specify)

7. Does your company host any cloud applications on purchased provider's storage , virtual machines, network services etc- (Infrastructure as a service)

*8. What are the Key steps you used in the migration of the application(s) to the Cloud (Eg, 1. gain access to Virtual machine,2. Deploy Operating system(Linux/window), 3. Install Apache server , 4. Patch OS and Apache server ,5. Use xxx to upload system to the cloud , 6. After upload enforce files access permissions,7. Setup DNS management 8. Test system components 9. Declare the migration process complete



9. Optional(Comment further on the best practices and key steps in migration of applications to the cloud):



10. Which IT technical skill sets do you find essential in the actual migration of IT-infrastructure to the cloud? (tick all that are that are useful)

- Systems Development skills
- Cyber Security skills
- Network administration skills
- Cloud infrastructure Skills
- General IT support skills
- Business Development skills

Customer service skills

Database administration skills

Other (please specify)



*11. How would you allocate roles and responsibilities to the various skill sets in Q10 above when performing the actual migration process?


Having all the skills in Q10 I would assign roles and responsibilities as follows:



*12. Which security policies do you deem necessary to implement on a hosted applications' cloud? eg (ACLs,VPNs,Authentication control, private public key encryption, hashes etc) name all that applies



13. What would be your advice to new technicians who want to gain the right skills in performing a future migration of systems to an Infrastructure-as-a-service offering?



Appendix 6: White box Testing Checklist

1. Standard coding practices have been used

Very satisfied Satisfied Not Satisfied

2. The style adopted is clean and clear when taken as a whole

Very satisfied Satisfied Not Satisfied

3. Concepts applied and their underlying ideas are expressed easily in plain language

Very satisfied Satisfied Not Satisfied

4. All functions have a clear place in the overall function of the whole, and are clearly expressed

Very satisfied Satisfied Not Satisfied

5. Code is well segmented and documented

Very satisfied Satisfied Not Satisfied

6. Code does not have redundant operations

Very satisfied Satisfied Not Satisfied

Stages in IaaS migration:

Company	IaaS Migration Stages								
	Access_V M	Deploy_ OS	Install_a pserver	Patch_OS _svr	Upload_f iles	Sec_polic ies	DNS_set up	system_t esting	declare_c omplete
Professional Digital Systems I	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
ITBrothers Limited	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
Kenya Airforce	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
TIM systems	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
GOK Database Admin	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
GoK	1.00	3.00	4.00	5.00	6.00	2.00	10.00	7.00	8.00
Indra Limited	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
Evamtech computer plus	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
UAP Holdings	1.00	2.00	3.00	4.00	5.00	6.00	7.00	10.00	10.00
SERVETECH SYSTEMS	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
NIBS	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
Impax Business Solutions	1.00	2.00	3.00	10.00	4.00	5.00	10.00	6.00	7.00
SEACOM	1.00	2.00	3.00	10.00	4.00	10.00	10.00	5.00	6.00
Kensoft Business Systems	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
Moi university	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
Kenya Private Schools Assoc	1.00	2.00	3.00	10.00	4.00	5.00	6.00	7.00	8.00
KEMU University	1.00	2.00	3.00	10.00	4.00	5.00	6.00	7.00	8.00
DKUT University	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
Fountain technologies	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
KWIKBET	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00
Solami Limited	1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00

Appendix 8: Some of the source Code Used

Authentication:

```
public function authenticateUser(LoginUserFormRequest $request)
{
    $email = nullable($request->email);
    $password = nullable($request->password);
    if (Auth::guard('user')->attempt(['email' => $email, 'password' => $password]))
    {
        return redirect()->route('App::dashboard');
    }
    else
    {
        return back()->withErrors('Email or password is incorrect.');
```

Error Handling, Password Hashing, Database Access:

```
// handle operation in a try-catch block for error handling
try {
    // use a DB transaction
    DB::beginTransaction();
    // fetch user from database
    $user = User::find($request->user_id);
    // assign them a new hashed password
    // hashed using bcrypt - very secure and one-way
    $user->password = bcrypt($request->password);
    // persist the changes to the DB
    $user->save();
    DB::commit();
    return redirect()->route('App::login_user')->withInfo('The account was setup
    successfully. Kindly login with the new password to gain access.');
```

Mail Sending:

```
// send email
Mail::to($user)->send(new NewProjectUserEmail($user, $project, $hash));
$info = "An email was successfully sent to ".$user->email.". Kindly have a look at
it in order to be able to activate your account.";
```

Logic Implemented:

```
$today = Carbon::now();
// check if user account activation token has expired
if($user->token_expires_at->gt($today))
{
    return view('App::auth.setup-account',compact('user'));
}
else
{
    // if expired, resend the account activation token
    $project = Project::find($project_id);
    if(isset($project))
    {
        return view('App::auth.resend-email',compact('user','project_id'));
    }
    else
    {
        return "Unable to fetch your project";
    }
}
}
```

New Project User Email Sending:

```
public $user;
public $token;
public $project;
public $url;
public function __construct($user, $project, $token)
{
    $this->user = $user;
    $this->token = $token;
    $this->project = $project;
    $this->url = route('App::setup_account',['email'=>$user->email,'token'=>$token,'project'
=>$project->id]);
}

/**
 * Build the message.
 *
 * @return $this
 */
public function build()
{
    return $this->
    subject('New Project Assigned!')->markdown('emails.new-project-user-email');
}
```


Documentation of Functions in Source Code:

```
546 /**
547  * Check if the logged in user is allowed to access a project
548  * @param int $project_id the ID of the project to be considered
549  * @return bool
550  */
551
552 function canViewProject($project_id)
553 {
554     // check if the user is logged in
555     if(Auth::guard('user')->check())
556     {
557         // fetch project
558         $project = App\Project::find($project_id);
559         if(isset($project))
560         {
561             // fetch the UserID of the logged in person (Laravel fashion)
562             $user = Auth::guard('user')->user();
563             $user_id = $user->id;
564             // check whether this logged in user is set as a user in that project
565             $project_user = App\ProjectUser::where('project_id',$project_id)->where('user_id',$
                    user_id)->first();
566             // if he is, thats fine
567             if(isset($project_user))
568             {
569                 return true;
570             }
571         }
572     }
573     // if not logged in, an automatic false
574     return false;
575 }
576 }
```

THE END.