A BYOD FRAMEWORK FOR SECURE USE OF MOBILE DEVICES IN UNIVERSITIES: THE CASE OF UNIVERSITIES IN KENYA

BY

DAVID K. NDENG'ERE

MASTER OF SCIENCE IN DATA COMMUNICATIONS

KCA UNIVERSITY

2017

A BYOD FRAMEWORK FOR SECURE USE OF MOBILE DEVICES IN UNIVERSITIES: THE CASE OF UNIVERSITIES IN KENYA

BY

DAVID KANYI NDENG'ERE

A DISSERTATION SUBMITTED IN PARTIAL FULLFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN DATA COMMUNICATIONS IN THE FACULTY OF COMPUTING AND INFORMATION SYSTEMS MANAGEMENT AT KCA UNIVERSITY.

NOVEMBER, 2017

DECLARATION

I declare that this dissertation is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this dissertation contains no material written or published by other people except where due reference is made and author duly acknowledged.

NAME: DAVID KANYI NDENG'ERE Reg. No: **14/02194**

Sign ……………………………………… Date ………………………………

I do hereby confirm that I have examined the master's dissertation of

DAVID KANYI NDENG'ERE

And have approved it for examination

Sign ………………………………………… Date ………………………..

PROF. PATRICK OGAO

Dissertation Supervisor

ABSTRACT

This project was to find out security threats, challenges and attacks brought about by BYOD adoption in institutions. Universities in Kenya as institutions of higher learning were chosen as a case study because BYOD was in extensive use and hence the threats, challenges and attacks would be more pronounced and frequent as compared to the non-academic institutions. The Threats, challenges and attacks were found out using a questionnaire that was sent to ICT administrators of 10 randomly sampled universities. Other existing frameworks were reviewed in order to find out how they tackled threats and challenges associated with BYOD. Framework as a BYOD solution was adopted for this study because the physical implementation of a BYOD solution in universities would be beyond the time limit of this project. The proposed framework was developed by modifying the BFS security framework and advanced it to include advanced devices access to the campus network, Malware detection and prevention, Mobile devices users' categorization and access to servers and rogue access points by disabling Hotspots applications in mobile devices. Simulation methodology (using OPNET version 14.5) was used to test and validate the proposed framework by subjecting the framework network model to a mobile attacker node and putting preventive measures to address the attack and then comparing the simulation results of the various aspects of network performance tested as well as the campus server that was being targeted. The sampled universities had not put adequate measurers to address the BYOD challenges and attacks they experienced and hence the proposed framework would be very useful if physically implemented.

KEYWORDS: BYOD, MDM, FRAMEWORK and Simulation.

ACKNOWLEDGMENT

I am grateful to my supervisor Prof. Patrick Ogao for his fruitful support and guidance to this project completion and success. His valuable contribution made it possible for me to achieve the objectives of this Project. May the Lord continue to enlarge his territories.

I thank my dear wife Jane Muthoni Kanyi for her patience, encouragement and moral support throughout the time I was working on this project. May the Lord bless you abundantly.

Above all I sincerely thank the Lord for giving me the room and capability to work on this project. May his name be glorified.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

BYOD	Bring Your Own Device
BYOT	Bring Your Own Technology
MDM	Mobile Device Management
VPN	Virtual private Network
FTP	File Transfer Protocol
3G	Third Generation
4G	Fourth Generation
MAUP	Multi Access User Policy
MVM	Mobile Virtual Machine
MAM	Mobile Applications Management
NAC	Network Access Control
SPD	Security Policy Database
NAS	Network Access Server
SSID	Service Set Identifier
WLAN	Wireless Local Area Network
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
IP	Internet Protocol
MAC	Media Access Control

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Bring your own device (BYOD) is an IT policy where employees, students, and other people are allowed or encouraged to use their personal mobile devices—and, increasingly, notebook PCs—to access enterprise data and systems. Today's students are already technology leaders. They want to take the technology they use in their daily lives and make it a normal part of their classroom experience. Research tells us that if we reflect this in their learning experiences, we will increase engagement, which leads to improved student success. As many IT departments struggle to keep up with yearly technology changes, company employees increasingly want to use their own devices to access corporate data.

It is part of a growing trend dubbed Bring Your Own Device (BYOD), which encompasses similar Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP) and Bring Your Own PC (BYOPC) initiatives. All of them have evolved to empower workforces through the so-called 'consumerization of IT'.

BYOD was coined by marketers to describe the consumerization of IT as the growth of home computing and new mobile devices that include smart phones and tablets led businesses to demand for simple and easier computing to match those used at home (Veen, 2014). Due to BYOD concepts in the industry, employees are able to use their own personal devices for personal use and work related activities for example to access the organization’s resources. With these concept organizations no longer desire to provision or maintain individual IT equipment instead that have left it to individuals to acquire their own devices which fall under their care. Some organizations provide incentives for individually owned devices while others do not.

BYOD enables individuals to be in charge of their own devices in relation to the operating systems, management and maintenance of the devices (Veen, 2014). According to Scarfo (2012) there are four different categories of BYOD adoption by organization:

(i) Here is your own: Everything is controlled, the enterprise provides devices and complete support.

(ii) Choose your own. In this case the enterprise provides a set of devices from which the users can choose from, policies are weaker and users are allowed to install selected software.

(iii) Bring your own: Corporate provides money to employees to buy devices on the consumer market, policies are weaker and people are allowed to install software as long they are compliant to some policies.

(iv) On your own: Bring anything, No support is provided, the device management is left to the employee.

There are some benefits brought about by adopting BYOD in organizations: Adopting BYOD reduces device investment costs for organizations by shifting the cost of procuring the devices to their employees (Calder, 2013). The other cost transferred to the employees by the organizations is that of replacing outdated equipment. Wood (2012) notes that employees get satisfied by owning their own devices since they are able to maintain and replace the device at own will. BYOD adoption also enables employees to use cutting edge technology due to their ability of being able to constantly upgrade their devices (Calder, 2013).

Another benefit to organizations due to BYOD adoption is increased productivity by employees since by using their own devices they are able to work outside normal office hours. Employees also appreciate more the IT support provided by their organizations since they perceive it as more personal instead of just support to the devices (Action learning project, 2012).

To enhance the benefits due to BYOD adoption several issues need to be addressed. These issues include challenges of delivering applications to multiple platforms, security issues (Scarfo, 2012) and privacy issues (Miller, Voas & Hulburt, 2012). According to Miller et al. (2012) the issue of employees’ privacy needs to be addressed because mobile devices contain a wealth of personal data which may mingle with employee data on the same device. It is very difficult to find a balance between strict security control for an organization’s data and privacy of personal data especially when the devices are not corporate issued assets; because both the organization and personal data coexist on same devices (Ghosh, Gajar & Rai, 2013). On the other hand Miller et al (2012) notes that there was a similarity between the BYOD initiative and the laptops introduction to organizations since the threats and security concerns associated with BYOD initiative are largely a replay” of those previously faced with laptops although the BYOD phenomenon is a tougher challenge to security because of the large number of devices.

Adoption of BYOD also initiates the fragmentation of devices and their security levels in organizations.Markel j& Bernik (2012) classified threats due to BYOD as direct threats like loss/theft of devices and indirect threats which include interceptions of communications due to unsecured wireless network, malware attacks and location tracking.

Other BYOD risks include; loss of control and visibility (Morrow, 2012; Miller et al,.2012; Thomson, 2012. An additional delicate risk of BYOD is that employees may abuse the technology usage and cause data leaks due to their unwillingness to backup data and their lack of awareness of their organization's security policies (Armando et al. 2014). Bandwidth is another key element to be taken into consideration since without enough bandwidth it is impossible to achieve mobility benefits (Scarfo, 2012). Lastly complying with contracts, law and even own policies is also a challenge (Navetta & Paschke, 2012).

Although BYOD introduces a new dimension towards security, Ernest and Young (2013) are of the view that BYOD risks and impacts are often the same to those experienced by organizations in normal information technology environment only that BYOD tends to expand the risk landscape with the potential of amplifying certain risks. For universities majority are adopting BYOD because their IT resources are insufficient to support their ever growing number of users and their fraternity member's ability to lay their hands on the most modern technologies due to the explosion of personal devices, smart phones, tablets, cloud storage and other individually owned technologies (Dahlstrom & Difilipo 2013). The BYOD trend in universities in Kenya is no different and it's attributed to the challenges of insufficient user per computer ratio and the ability of faculty, staff and students seeing tremendous value in the integrating these personally owned technologies with institutional systems and resources (Karshoda & Waema 2014).

1.2 Problem Statement

Security of IT resources is a key requirement for any organization including universities. However, to put in place holistic security measures for all known IT security challenges is expensive and beyond the reach of many universities (Dahlstrom & Difilipo, 2013). Therefore, the most effective approach for universities in Kenya to address the expanded IT security risk portfolio arising due to BOYD adoption is by them putting in place security measures that specifically address identified known as BYOD security challenges. According to (Boon & Sulaiman, 2015) the current models from various experts are meant to address specific issues and challenges (highlighted in section 2.4) and to make them work for broad BYOD scenarios then modification of these models to produce a single suitable model that can address all BYOD security issues in an enterprise is needed.

The proposed model will therefore be modified from existing models to meet BYOD security challenges faced in Universities in Kenya as a case of study. The benefits that universities in Kenya expect to rip due to BYOD adoption may be eroded as a result of expanded IT security risk portfolio due to BYOD adoption. Universities like any other organization have tried to safeguard their information from attacks; they accomplish this by following common procedures and techniques that may be inadequate without reference to a suitable model that can guide them.

This study seeks to address this gap by developing an effective BYOD security model that universities in Kenya may refer to as they put in place security measures to address these emerging security challenges due to BYOD adoption that are not addressed by the current models and to safeguard themselves from such threats.

1.3 General Objective

To review BYOD security frameworks currently available and develop a better framework that universities can adopt to securely adopt BYOD and in return rip full benefits brought about by BYOD.

1.4 Specific Objectives

(i) To review security challenges due to BYOD adoption facing universities in Kenya and measurers put in place to tackle them.

(ii) To review existing BYOD security frameworks.

(iii) To develop an advanced devices access BYOD security frameworks that will guide universities to securely adopt BYOD.

(iv) To test and validate the framework.

1.5 Research Questions

(i) What are the emerging security challenges due to BYOD adoption facing universities?

(ii) What are the security measures that have been put in place by universities in Kenya to address emerging security challenges due to BYOD adoption?

(iii) Is there a BYOD security framework that guides universities to securely adopt BYOD?

(iv) Will the developed BYOD security framework be suitable and better than existing frameworks to guide universities to securely adopt BYOD?

1.6 Significance of the Study

This study is meant to generate up to date empirical data sets on challenges facing universities in Kenya due to BYOD adoption and the security measures that the universities has put in place to address those challenges. By referring to this empirical data sets universities in Kenya will be able to effectively put in place security measures that will address the emerging security challenges facing them due to BYOD adoption.

The proposed BYOD security framework will provide universities with a well-structured guide on how to put in place BYOD security measures. Well managed security will enable universities to rip maximum benefits due to BYOD adoption.

1.7 Justification of the Framework as a Solution to BYOD Security Threats And Challenges

A BYOD framework is a systematic model and related processes to resolve each component issues holistically. Frameworks act as guidelines in implementing solutions to BYOD security challenges. The actual solution to the BYOD challenges in the institutions of higher learning where BYOD is in intense practice would take long to implement physically which would hinder the completion of this project.

A BYOD framework will therefore give clear guidelines to the processes and components that will be involved to achieve the intended solutions to BYOD security challenges. The framework is clearly illustrated and designed in order to model the actual implementation of the BYOD security challenges solutions in institutions of higher learning (universities being used a sample).

The framework components will be tested using simulation methodology in order to test and validate the framework for physical implementation in universities. The proposed BYOD framework can therefore be physically implemented on the institutions of higher learning to achieve the desired goals and solutions to BYOD security challenges.

CHAPTER TWO

LITERATURE REVIEW

2.1 BYOD Overview

With mobile devices increasingly embedded into all parts of our personal lives, organizations are finding that their employees increasingly want to use their own personal mobile devices to conduct work (often alongside corporate-provided devices), and many are reaching out to corporate IT to support this. Employers have concluded that they can't physically stop the use of mobile devices for both work and personal agendas, but they need to know how to control it. In the current economic environment, companies are demanding that employees be more productive: having a robust mobile program that allows personal devices to be used safely in a work capacity can raise employee productivity and be a significant competitive advantage. Employees IT ownership model, typically called bring your own device (BYOD), presents an attractive option to organizations.

BYOD significantly impacts the traditional security model of protecting the perimeter of the IT organization by blurring the definition of that perimeter, both in terms of physical location and in asset ownership. With personal devices now being used to access corporate email, calendars, applications and data; many organizations are struggling with how to fully define the impact to their security posture and establish acceptable procedures and support models that balance both their employees' needs and their security concerns.

Drivers of BYOD adoption include technology savvy workforce who are able to lay their hands on sophisticated devices than those provided by their organizations (Pricewaterhouse Coopers, 2013), generational shift in the expectations of employees who demand job flexibility of working from anywhere (Devine, 2012; Thomson, 2012) and the possibility of technically shrinking the many devices used by employees for both work and home purposes into one (Miller et a1, 2012). Various surveys carried out indicate that BYOD is increasingly being adopted by organizations including academic institutions. In a survey of 600 IT leaders by Cisco, 95% of the companies indicated that they already permitted some form of BYOD in their organizations (Cisco, 2012).

In a survey of universities in Kenya carried out in 2013, 53% of students owned laptops while 53% owned smart phones (Karshoda, 2014). Thus the popularity of mobile devices in workplaces and campuses cannot be overlooked. For universities in Kenya the trend has been due to staff and students seeing tremendous value in integrating personally owned technologies with institutional systems and resources (Karshoda, 2014).

According to Tom Murphy of Bradford Networks "education institutions have been at the forefront of the BYOD trend for years and in many ways provide a roadmap for organizations that are just starting to embrace freedom of device choice for their employees"(Info Security, 2013).The other driver for BYOD adoption in educational institutions has been due to the ability of university's fraternity members to lay their hands on the most modern technologies (Dahlstrom & Difilipo, 2013), the tight budget and resources shortfalls that institution leaders struggle with which leaves them unable to afford school-owned devices for students and staff at a time when demand for them is increasing rapidly (Issue Brief, n.d).

2.1.1 BYOD in Kenya

According to the research conducted by Jane Arwa for her MBA project at University of Nairobi she noted that BYOD was in use at KCB bank for enhancing customer service delivery. BYOD in Kenya has been fronted by competition in the mobile telecommunication industry that has seen its market leader Safaricom partnering with different organizations to push up the demand for the devices and its 25.1 million subscribers (according to the report released by CAK on June 26, 2016) on 3G network and currently 4G network e.g Laptop for ALL students where it worked with local universities and banks to avail cheap devices to students, it also partnered with mobile phone producers and electronic giants i.e Samsung and Intel and has already rolled out a plan to abandon feature phones in favor of affordable smartphones. This move has seen it sell smartphones at prices lower than the market average. These devices have found their way into the work place and as revealed by William (2013) and Etale (2013), BYOD is practiced even if not sanctioned officially by management (PwC, 2012)

2.1.2 BYOD around the World.

This theme discusses Bring Your Own Device as a concept by critically looking at a conceptual paper and a research paper namely**;** Bring Your Own Device; The emerging trend in more ways than one Drury and Absalom, (2012) and Bring Your Own Device; The Unstoppable Phenomenon (Unisys 2011) and others. A longitudinal study conducted by (Unisys, 2011) found out that employees wanted to use different products than what the organization was buying. According to the chief information security officer at Unisys, It was a huge paradigm shift. They wanted to buy the devices they were most comfortable with, hence BYOD. The concept was regarded as unstoppable and was hitting businesses worldwide. Devices and services historically available only in the workplace and provided by IT departments are now widely available to and affordable by consumers (CIO, 2011).

The introduction of devices such as the Apple iPhone and iPad, Google Android smartphones and tablets, and lower cost laptops and recent explosion in technology “consumerization” of IT has increased consumers’ appetite for the latest technology, and they crave that same technology at the workplace (Cio, 2011), (Slottow, 2012). With this widespread adoption of myriad consumer mobile devices including all flavors of 14 smartphones and tablets combined with a growing number of employees who are accustomed to using them, companies must figure out ways to accommodate them.

This was also agreed by a research paper (Accenture, 2011) that expounded that it is mandatory to address employee demands for accessing corporate data without forcing them to carry two different mobile devices, one for work and one for personal use. It also means addressing their demands to avoid carrying two different mobile devices, one for work and another for personal use.

2.2 Security Threats and Challenges in a BYOD Environment

Despite the benefits, adopting BYOD in organizations creates potential security concerns due to user devices having access to organizations internal IT resources (Moreira et al., 2015). Security concerns due to BYOD affect both the organizations and their employees. Mobile devices expand the scope of risk to an institutions information security due to their Wireless capability. Security threats on wireless networks are on the constant rise (Kim & Hong, 2014).

Gartner report of 2013 notes that employees bring their own devices and connect to the enterprise network for access of data without consideration of the information security. (Kim & Hong), 2014 identifies malware attacks through rogue access points provided by an attacker as the major security threat in a BYOD environment. They further note that wireless connection environment in a smart device can easily be attacked as compared to a conventional computer environment when exposed to a malicious code attack as result of visiting a harmful web site.

Some of the noted potential threats through mobile applications are data leakage, denial of service attack and charging damage (Ghosh et al., 2013). They note that the risk of data leakage is very severe since mobile devices are designed to access the cloud for data sharing and have no general purpose file system in business to share.

Charging damage is a result of no clear separation of personal and cooperate data held in mobile devices. Cisco 2014 annual security report highlights BYOD threats as: High Threat Malware, hijacked infrastructure, sites without content, suspect FTP and suspect VPN.

Figure 1 illustrates the challenges of adopting BYOD according to a survey conducted by ESG in 2013 to IT professionals.

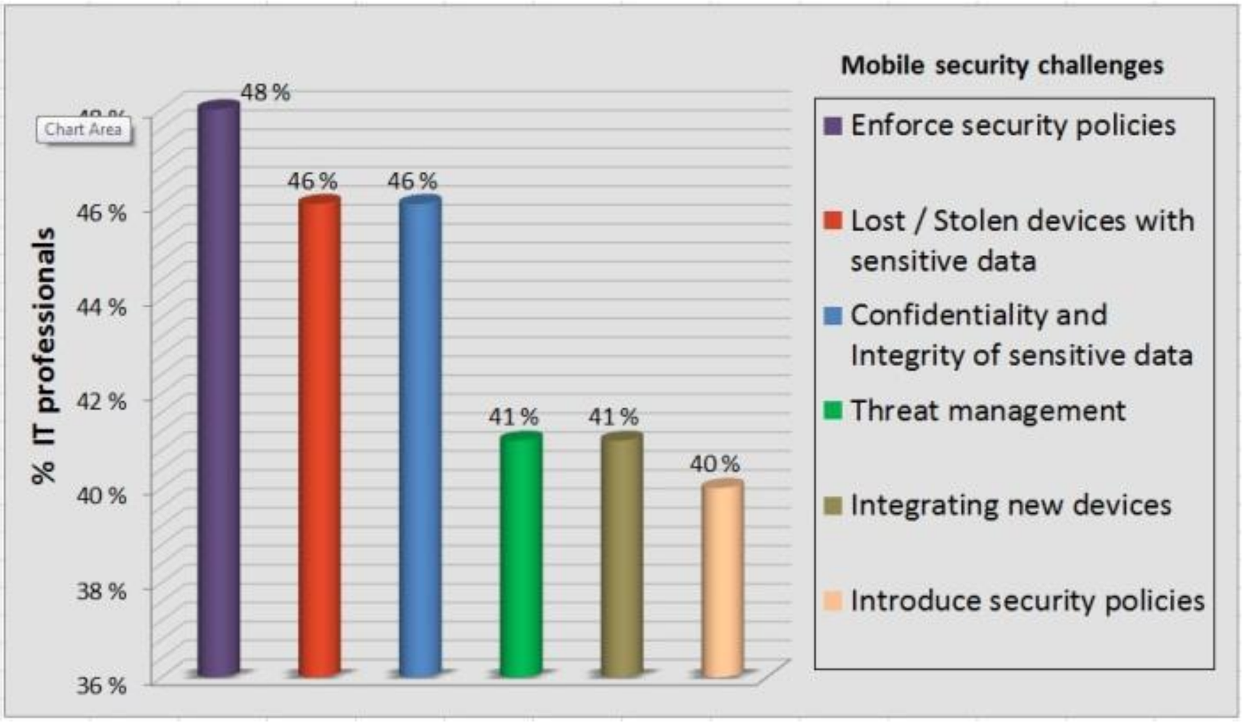


Figure 1: BYOD security Challenges Source: ESG research survey- Ghosh et al., 2013

The biggest contributor to the security challenges brought about by mobile devices is their extra portability which in turn poses a great challenge of loss of information in case of loss or theft. Mobile devices may not be sophisticated in terms of security issues: firmware updates, patches, anti-virus and configuration settings and hence they expose the enterprise network to threats. Mobile devices use variety of mobile operating systems which keep on advancing technologically and hence the already installed OS become outdated very fast (Ghosh et al., 2013).

2.3 Technological Measurers Adopted to tackle BYOD Security Threats and Challenges

Various BYOD security researchers have developed BYOD frameworks that act as a guide of implementing specific BYOD security measures. The frameworks will reviewed and critiqued in the section 2.4. Due to the threats introduced or expanded by the mobile devices the industry has developed technological solutions to address specific challenges highlighted in section 2.2. The main technological solution in the industry is the Mobile Device Management (MDM) solution.

2.3.1 Mobile Device Management (MDM)

MDM tools give aid to the institutions by controlling the mobile devices that are in connection to their local network. With the aid of MDM tools institutions are in a position to lock down the mobile devices, encrypt the stored data or even wipe out the data locally or remotely and enforce policies on the connected device. The MDM tools address the issue of security by monitoring, controlling and protecting the device via: enforcing security settings, managing passwords, installing digital certificates for authentication and monitoring installed applications.

In managing devices the MDM tools can generate a report of connected devices and their applications. They also have the capability of profiling the devices and files in them. MDM tools restrict the user to download and install certain applications that do not meet the security requirements. MDM tools offer data backup and offer recovery services (Ghosh et al., 2013).

An additional feature of MDM tools highlighted by (Herenandez & Choi, 2014) is the creation of a secure container which overcomes the inherent weaknesses present in Android operating systems, which offer no inherent encryption or automatic access control. Implementation of the MDM tools on an enterprise network is not easy due to the client to server relationship that exist in enterprises- devices between clients and server such as firewalls, servers, proxies, active directory etc.

There are various MDM tools in the market each with various features and capabilities. Strom, 2013 reviewed six of the most popular MDM solutions:

- Airwatch
- Apperian EASE
- BlackBerry Enterprise Server 10 (BES10)
- Divide
- Fixmo
- Good Technology's Good for Enterprise

He noted the following about some of the above MDM solutions:

Good Technology’s product has a strong secure container and is fast and easy to deploy, but it has weak application and file control.

Divide is the best in terms of deployment ease and features, but it only supports iOS and Android devices.

AirWatch seems to be the most complete product with a separate MDM, a mobile content or file management, and mobile application control service, each managed by a single, integrated console delivered from a cloud or on the premises.

MDMs alone are not enough. MDM has to be accompanied with a strong forward-looking MAUP, network tools that allow network managers to control bandwidth utilized by these devices in order of their priority, securing the network, controlling who gets access through automated device recognition, and recognizing when devices have been jail broken or rooted so that these devices are denied access. Additional accompaniment to the MDM tool is the Network Access Control devices (Clarke, 2013).

2.4 A Review of Current BYOD Security Frameworks

To address BYOD security challenges and issues different BYOD frameworks and other solutions are proposed by various security experts to mitigate different issues. A BYOD framework is a systematic model and related processes to resolve each component issues holistically. The current BYOD frameworks were reviewed based on their existing literature and against the listed goals.

In order to prevent BYOD threats and challenges, a BYOD solution must achieve the following goals: (Ocano, Ramamurthy and Wang, 2015)

- Space isolation, by separating the corporate's space from the employee's space so that different security policies can be enforced.
- Corporate data protection, by employing encryption and rejecting unauthorized access.

- Security policy enforcement, where the mobile device complies with the corporation's security policies.
- True isolation, where the corporate's data is not located on the BYOD device.
- Non-intrusive, meaning that any software installed in the mobile device must not need any special privilege that might allow it to monitor the behavior of the user on his or her device.
- Non-resource-intensive, as mobile devices are resource constrained and do not have much spare resources for demanding applications.

2.4.1 Related Work

BYOD is an area where a lot of research has been conducted on to come up with frameworks and other solutions. Ocano, Ramamurthy and Wang, (2015) categorized the various BYOD solutions into 5 categories as follows:

- Agent Based
- Cloud Based
- Mobile Virtual Machine(MVM)
- Framework
- Trusted Execution Environment (TEE)

Leavitt (2013) elaborated on the Mobile Device Management and Mobile Applications Management (MAM). He noted that MDM/MAM are agent-based because an application must be installed in the employee's device to allow the enterprise to lock down, control, encrypt and enforce policies. With an MDM, the enterprise can control the behavior, data, and applications installed in the BYOD device; while an MAM only focuses on managing applications. He also elaborated on the cloud based solutions as solutions that rely on cloud storage to provide mobile access to data and applications. They create space isolation but once the data is downloaded, data isolation is lost.

Additionally, they do not offer policy enforcement. Wang et al. (2014) elaborated on the use of Mobile Virtual Machine (MVM). According to them MVM solutions separate spaces in the mobile device, as they can use one Operating System (OS) for the user and another for the enterprise. There are two types of virtual machines for mobile phones: heavy duty and simplified lightweight. The former allows the user to install multiple OSs, while the latter needs less resources but it does not allow the user to install multiple OSs. Russello et al. (2012) developed MOSES, a policy based framework for enforcing software and data isolation on the Android platform, using a lightweight approach.

Andrus et al. (2011) developed Cells, a lightweight Virtual Machine (VM) architecture for mobile phones based on Android platform. Titze et al. (2013) proposed a Security Service Architecture (SSA) for security checks of smartphones that replicates the employee’s smartphone on the enterprise side and analyzes it to find security flaws. Chung et al. (2012) developed 2TAC, which addresses access issues by using a double layer access control (one at the device and the other in the cloud) along with device security profiles, anti-virus/malware scanners, and social networking.

BYOD Security Framework (BSF) was proposed by Wang et al. (2014). In this framework, there is an enterprise side that includes the corporate’s resources, a Security Policy Database (SPD), an MDM, as well as a Network Access Control (NAC) that separates requests coming from the personal space or corporate space based on the policies from the SPD. Additionally, there is a BYOD side where isolation is present by implementing an MVM. In the corporate space, there is an MDM agent that enforces the security policies in the corporate data.

The corporate space includes cryptographic primitives that make the enterprise's data confidential to non-enterprise actions. This framework provides data protection, isolation and policy enforcement, but at the expense of installing an MVM and an MDM agent in the BYOD device. Cisco (2013) offers

BYOD Smart Solution which focuses on the infrastructure of the network and provides policy management, mobility and applications, while supporting MDMs from third parties. Ekberg et al. (2013) elaborated on TEEs, which separates the execution of an application into secure and insecure parts by using a protected area in the processor. Zhao, Osono (2012) developed TrustDroid, an Android application that analyzes other applications, to prevent them from accessing the corporate data. TEE provides space isolation but data can be stored in the mobile device and it does not offer policy enforcement.

2.4.2 Comparison between The Different Types Of Solutions

This section will review the different types of solutions by comparing them to the desired goals of a solution or a framework.

		DESIRED GOALS					
Solution	Type	Space Isolation	Security Policies	Corporate data protection	Non-intrusive	Non resource intensive	True Isolation
MDM/MAM	Agent based		X	X		X	
Cloud-based	Cloud Based			X	X	X	X

MOSES	MVM	X		X			
CELL	MVM	X		X			
SSA	Framework		X				
2TAC	Framework		X				
Cisco	Framework		X		X	X	
BSF	Framework	X	X	X			
TrustDroid	TEE	X	X				
KANYI BYOD Framework	Framework	X	X	X		X	X

Table 1: Comparison between the Different Types of Solutions

CHAPTER THREE:

METHODOLOGY

3.1 Introduction

This section on methodology highlights methods, tools, and strategies used for data collection and data analysis. Subjects discussed in this section include research design, types of data, sampling, data collection, data analysis and ethical consideration.

3.1 Research Design

This is defined as the strategy, the plan and the structure of conducting a research project (Carriger, 2000). This study intends to use an exploratory case study research design and the reasoning is because the BYOD concept is not as clearly defined, understood or explored within the Kenyan context. Babbie and Earl (2007) stipulate that the main goal of an exploratory research design is to provide insights into, and an understanding of, the problem confronting the researcher.

The exploratory case study research design will help gather as much information as possible to make generalizations that best fit the population. The researcher aims to conduct a case study through use of questionnaire on ten universities in Kenya. These ten universities form a good representative of the higher education institutions in the country.

3.2 Data Collection

An extensive literature search using the WorldCat search engine with the search terms: Bring

Your Own Device, BYOD, BYOT, BYOS, Bring Your Own, office-home smartphone, smartphone+information management, smartphone+policy, personally owned, consumerization, shadow IT and mobile computing, in combinations with information management, policy, security management, private, privacy, user-driven and dual-use. The search was filtered for peer-reviewed articles in English.

Sample frame

The sample frame for the study was higher learning institutions.

Sample size

The researcher targeted ten higher learning institutions. The ten institutions are a representative of the university population in Kenya. The researcher used simple random sampling to identify the ten higher learning institutions. Simple random sampling allowed all universities to stand a chance to be selected to participate in the study.

3.3 Data Analysis

The process of data analysis will involve various stages. The nature of the data will be both qualitative and quantitative. Completed questionnaires will be edited for completeness and consistency. The data will be coded and checked for any errors and omissions. Responses from the questionnaires will be tabulated and coded. Qualitative data will also be analyzed through content analysis.

According to Mugenda and Mugenda (1999), content analysis is used to determine the presence of certain words or concepts within texts or sets of tests. Researchers quantify and analyze the presence-meanings and relationships of such words and concepts, then make inferences about the messages within the texts, the writers(s), the audience, and even the culture and time of these are a part.

3.4 Questionnaire Methodology to Achieve Objective 1

The objective 1 was to be best achieved via the questionnaire methodology that targeted ICT administrators in both public and private universities. The researcher wanted to get the actual challenges faced by universities as a result of adopting BYOD and actual measurers that were adopted by the sampled universities to address the challenges and hence the use of the questionnaire.

The challenges gathered and local solutions in place aided in the development of the framework. Kenya has got 22 public universities and 14 chartered private universities. Simple random sampling technique was used to come up with a sample size in order to give each university an equal chance of being chosen. The lottery method of random sampling was used to pick the desired sample size of 10 universities. All the universities were allocated numbers and 10 numbers were then randomly picked. The questionnaires were then sent by email to the ICT administrators of the 10 picked universities.

3.5 Simulation Methodology to Test and Validate the Proposed Framework

The proposed framework was tested for security vulnerability using simulation methodology. This was done in order to achieve objective 4. The simulation tool used was OPNET (Optimized Network Engineering Tool) version 14.5. This tool was chosen because it was powerful and versatile in the area of network simulation.

Simulation methodology was adopted because it would be too much time consuming to physically implement and test the proposed framework. Simulation would therefore act as very useful methodology of designing the framework components and testing in order to validate the framework. The proposed framework components were designed in OPNET and an attacker node was introduced in order to test the vulnerabilities or performance of the framework.

3.6 The Development of the Framework

The proposed BYOD security framework will be adopted and modified from the BSF framework that was highlighted in section 2.4.1. The BSF framework fell short of addressing some critical security threats and challenges that are highlighted below:

- Device access to the enterprise network-an elaborate and secure access of mobile devices into the campus network.
- Malware invasion-malware installed into mobile devices with an aim of attacking internal systems and other mobile devices.
- Rogue access points, WLAN adhoc functions in smart phones and hotspot applications in laptops- disabling of WLAN adhoc-tethering and hotspots in smart phones and hotspot applications such as connectify in laptops to avoid unauthenticated connection of other mobile devices through the authenticated ones.

The proposed framework will therefore address the above gaps by applying advanced devices access procedure to the campus network. This will be achieved by the MDM agent installed by the MDM server to the devices and Network Access Server (NAS). The MDM agent will be advanced as compared to the BSF model. It will monitor and handle security issues at the BYOD side therefore ensuring that the enterprise side is safe. Unlike the BSF model the proposed model will introduce Mobile Devices Firewall that ensures that users only access the desired campus resources.

BSF model makes use of MVM for space isolation. MVM is a second intrusion to the device and therefore the proposed model will make use of MDM agent to create a secure container (encrypted) to store data that is downloaded from the enterprise servers and emails.

This data will be wiped out by the agent when the device becomes inactive or is out of range of the campus Wi-Fi range.

The description and structure of the proposed model starts from section 3.7 below

3.7 The Proposed Kanyi BYOD Framework

The biggest disadvantage of the proposed framework is that it is intrusive- the owner of the device has to install the MDM agent that is sent from the MDM server. In reference to its Architecture the model is divided into 2 parts just like the BSF model:

BYOD Side: this is the device side. The BYOD side is entirely monitored by the installed MDM agent. The MDM agent is the key security implementing feature at the BYOD side. It scans the device to ensure that it is safe to be granted access by the NAC server located on the enterprise side. It monitors applications to ensure that they do not introduce malwares into the campus network.

The agent disables Adhoc networking (tethering and hotspot applications) in mobile devices and other SSIDs while the active campus SSID is still active in order to avoid rogue access points. It’s a requirement for the MDM agent to be installed in the device before permission to access the campus network can be granted by the NAC server. The NAC server has to get permission granted confirmation from the agent before granting a device access to the campus network.

Enterprise Side: This is the side of the campus network consisting of the rest of the elements of the KANYI BYOD framework. The elements will be discussed in detail in the section below. The elements consist of:

- Network Access Server (NAS)

- MDM server and Console
- Campus Firewall
- Mobile Devices Firewall
- MDM gateway server.

KANYI BYOD framework will aim to achieve the following specific goals that are related to threats and challenges of adopting BYOD:

- Device access to the enterprise network
- Separation of personal and corporate data on the device
- Malware invasion
- Management of the devices.
- Security of the campus temporary stored data.
- Ensuring the device OS is updated and secure and antivirus is installed and updated.
- Controlled access to internal systems and servers.
- Rogue access points, WLAN adhoc functions in smart phones and hotspot applications in laptops.

3.7.1 Description of Kanyi BYOD Security Framework:

- Secure access: Centralized log in system—Network Access Server NAS server) and DHCP server. Checks for username and password of a user fed from the mobile device and delivered to the NAS server by the Access Point. Identify a user as student, non-teaching staff (ICT administrative staff, administrative assistants and senior administration staff) and teaching staff. Once the credentials go through, the NAS passes the details of the user (category of user, type of device and MAC address of the device) to the MDM server. Upon successful authentication the device is issued with an IP address by the integrated DHCP server so as to enable MDM server install the MDM agent in the device.

- Mobile Devices Management- MDM server and MDM Agent. This server is responsible for check-up of mobile devices through the agents. Once a device is authenticated through the NAS server and assigned an IP address, The MDM installs the agent to the device (user is prompted of the installation-accepts or rejects-if the user rejects he is logged out by NAS server and no more connection). Scanning of the mobile device by the agent takes place to verify whether the device can be trusted (check the OS version and vulnerabilities, antivirus in use-current, insecure applications installed-only trusted applications will be granted access). Once the device is trusted it is added to the trusted list in the MDM server and the owner of the device, type of device and its MAC address are noted. Details of active and permitted applications on the mobile device are captured by the agent and permitted to send and receive data through the campus network. Any insecure or denied application is blocked by the agent and the owner is notified. Categorization of users by the MDM server also takes place and Mobile Device Firewall denies or permits access to internal systems and server: students' devices are permitted access to the internet, student's portal and e-learning portal. Access to the internal systems' servers is denied. Non-teaching staff access depends on the kind of systems they access and use to execute their tasks. They will therefore be granted access to the system(s) they use and downloading or exporting of the university data to their personal devices will be permitted. University data will however be stored in a secure container (encrypted) created by the agent and wiped out immediately the campus WI-FI connection is lost or disconnected. Attachment of university data to any other email domain will be denied by the agent. Internet access will be additionally granted to the non-teaching staff. ICT administrators will be granted access to the servers and systems they administer and manage only besides the internet access. Senior university administrators such as deans, registrars, DVCs and VC have access to the internet and the specific university systems they may need access to with exporting or downloading university data to their personal devices allowed but with same restrictions stated above. Teaching staff have access to the internet, faculty portal, e-resources and e-learning systems only. Any device that does not pass the trust test (performed by the agent) is added to the MDM server untrusted list together with its owner details and MAC address and is therefore blocked and is logged out by the NAS server. The MDM agent notifies the owner of the device of the reason of denial of access to the campus network and recommends the appropriate action to be taken by the owner of the device before attempting to connect again. A mobile device that is connected but inactive is immediately disconnected by the NAC server following request from MDM agent.

- Mobile Devices Firewall-MDM server is connected to the Mobile devices firewall so as to deny or permit the data traffic to the mobile devices based on the type of user, permitted applications and internet activity of the user. Mobile devices firewall is further connected to the main university firewall for external data traffic filtering.
- MDM Gateway server- Located at the DMZ zone and communicates with the MDM server so as to filter incoming and outgoing traffic from mobile devices.

- BYOD policy- The universities have to develop a BYOD policy to which all the mobile devices must comply to before and during the connection with the university network.

3.7.2 Kanyi BYOD Security Framework Data Flow Diagram for Device Access to the Campus Network

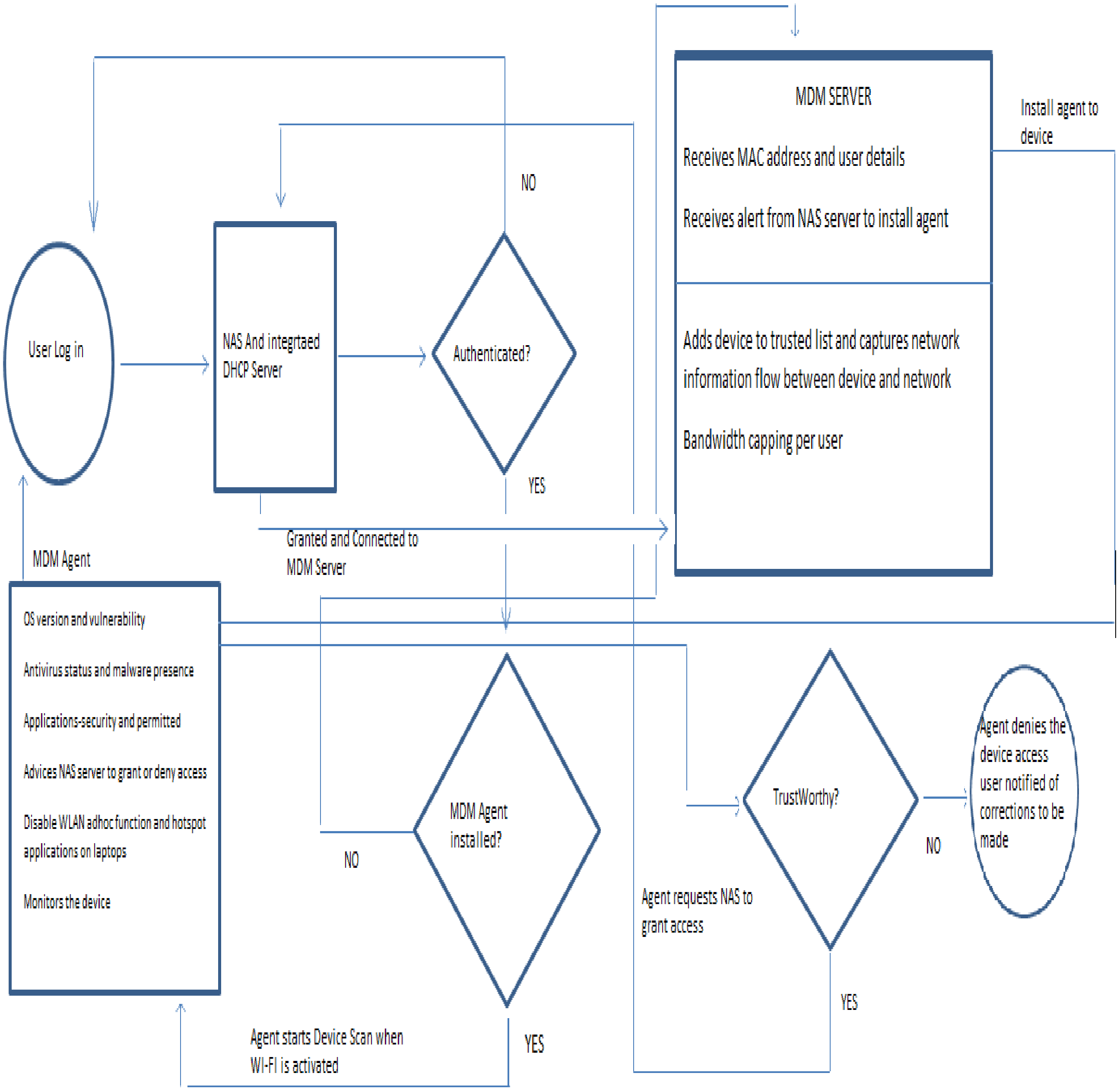

MDM SERVER
Receives MAC address and user details
Receives alert from NAS server to install agent
Adds device to trusted list and captures network information flow between device and network
Bandwidth capping per user
Install agent to device
NO
User Log in
NAS And integrtaed DHCP Server
Authenticated?
YES
Granted and Connected to MDM Server
MDM Agent
OS version and vulnerability
Antivirus status and malware presence
Applications-security and permitted
Advices NAS server to grant or deny access
Disable WLAN adhoc function and hotspot applications on laptops
Monitors the device
MDM Agent installed?
NO
TrustWorthy?
NO
Agent denies the device access user notified of corrections to be made
Agent requests NAS to grant access
YES
Agent starts Device Scan when WI-FI is activated
YES

Figure 2: KANYI BYOD Security Framework Data Flow Diagram for devices access to the Campus network.

3.7.3 General Outline of the Kanyi BYOD Security Framework

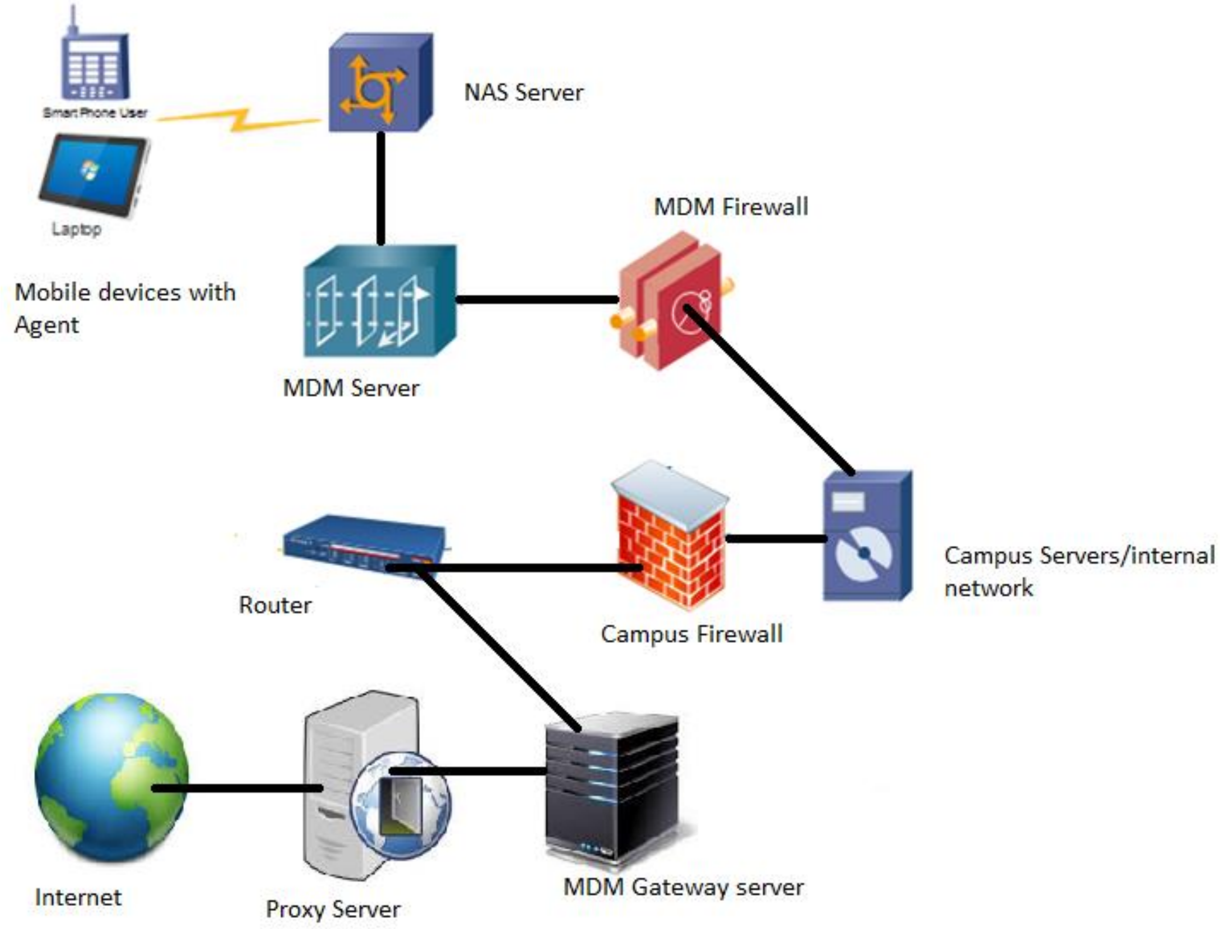


Figure 3: General Outline of KANYI BYOD Security framework

3.7.4 Functional Performance of the Kanyi BYOD Framework Components.

Model Component	Functions	Specifications	Connection
Mobile device	Device through which a user connects to the campus network.	Laptop and MAC Book (running windows, Linux or MAC OS). Tablet and smartphones/Iphones/windows	Through the Access Point.

		phones (running Android, windows, and IOS)	
Access Point	Mobile devices connect through it to the campus network	Runs on WI-FI standards: 802.11 b/g/n and ac. Uses WPA 2-Enterprise security standard.	Connects to the NAS server for authentication of users and issue of IP address.
Network Access Server and DHCP server	Offers centralized authentication to the network and systems. Gives mobile devices access to the campus network. Alerts the MDM server of connection of mobile devices. Sending request to MDM server to install MDM agent in the device if not installed-keeps record of MAC address and whether agent was installed on the device. DE authentication and logging out of users. Categorization of the campus users. Captures the MAC address of the device. Integrated DHCP server to assign IP addresses once the device is	Server runs the centralized authentication system-Windows Active Directory authentication system or RADIUS server. Server runs Network access system-captures details of device-MAC address and IP address, alerts the MDM server of a device connection in order for MDM to install agent on the device, sends MAC address and IP address of device to the MDM server, forwards and receives traffic from agent and MDM server and grants or denies device access to the campus network. DHCP server to assign IP addresses once authentication is performed.	Connects to the Access point and MDM server.

	authenticated. Forwards and receives traffic from the MDM agent and server.		
MDM Server	Capture of the details of all connected devices-monitoring of connected devices through MDM agents. Send of DE authentication and log out request to the NAS server.	MDM server system installed to a computer of good hardware specifications-memory, hard disk and processor speed. MDM server system is accessed by administrator through the MDM console installed on a desktop computer/laptop.	Connected to the NAS server. Connects to the Mobile device Firewall.
MDM Agent	Scan of the mobile devices for OS versions, types and vulnerabilities, antivirus status and applications. Trusted device is permitted to connect while untrusted device is denied access till the MDM agent recommendations to the user are acted upon. Communicates with the MDM server-sends trusted device details (OS version, type of device and installed applications). Allows download and upload of university data to	MDM agent is installed on the mobile device after authentication by the NAS server is successful, device issued with an IP address and details of the user and MAC address are sent to the MDM server. User is prompted to install the agent on the first time device log onto the campus network. On the subsequent connections the MDM agent starts background scan of the device upon receiving the campus WI-FI signal, communication to and from the MDM server starts after authentication is performed by the NAS server. Device is fully connected and can send and receive data after the scan by the agent is complete. If the device violates policy or is inactive the agent alerts the MDM server to disconnect the	Connects to the MDM server through the access point and NAS server.

	and from official email domain only and permitted systems but agent wipes the data once the device is out of reach of campus WI-FI signal. MDM agent disables an ad hoc WLAN function on the authorized connected device so not to connect unauthorized device. It also disables hotspot applications installed on laptops in order to prevent unauthorized connection to the campus network. Monitors the device for installation of malware and other applications while connected.	user through the NAS server.	
Mobile Device Firewall	The device based firewall denies/permits devices access to the internal servers/systems based on user categorization received from the MDM server.	The device contains the mobile firewall software that ensures secure communication between the mobile devices and campus network.	Connects to the MDM server and the Campus server room.
MDM Gateway Server	Provides a network access point for managed BYOD devices when in connection to the	This server is outside the campus firewall. It reads from the MDM server so as to filter incoming and outgoing traffic from mobile devices.	Connected to the proxy server and campus firewall

	internet. It filters the outgoing and incoming traffic to and from mobile devices.		

Table 2: Functional Performance of KANYI BYOD Security Framework Components

3.7.5 BYOD Security Challenges that Kanyi BYOD Security Framework will address.

BYOD Challenge	Model component to address	Mechanism of Addressing the challenge
Insecure mobile device Access to the Campus network	NAS Server and MDM agent	Granting access through centralized authentication system-NAS server. Disconnects mobile device from the campus network once it becomes inactive, violates policy or is infected by a malware request from MDM agent to MDM server; then MDM server to NAS server. NAS server checks the device for the presence of the MDM agent; if not installed it requests the MDM server to install MDM agent. No device is permitted to access the campus network without the installation of the MDM agent. MDM agent scans the device and is only granted access after agent is complete with scan. Association of users to their devices-sends these details to

		the MDM server. MDM agent disables an ad hoc WLAN function on the authorized connected device so not to connect unauthorized device. It also disables hotspot applications installed on laptops in order to prevent unauthorized connection to the campus network. MDM agent only accepts connection to the authorized campus SSID and disables the other SSIDS while within the campus.
Keeping devices Operating systems and Applications updated and secure. Outdated or lack of mobile antiviruses on the mobile device. Installation of Malware into mobile devices.	MDM agent MDM Agent and Antiviruses	The MDM agent is tasked with the responsibility of ensuring that OS and applications are updated to avoid vulnerabilities and insecurities associated with them. A device with an old version of OS that has vulnerabilities or applications that are outdated and vulnerable is not granted access to the campus network. MDM agent scans and ensures that the device has an effective and updated mobile antivirus program before being granted access to the campus network. MDM agent will closely monitor all applications installations into the device and will only permit the application to run if it is secure and not have malware characteristics.
Tracking and accountability of connected mobile devices.	MDM server through agents.	MDM server through agents keeps track and account for all connected devices and

		activities happening in them.
Controlling mobile devices access to the campus network-internal network.	Mobile Device Firewall	Mobile devices have controlled access to the campus systems and servers based on user categorization fed to the mobile device firewall from the MDM server.
Campus data on personal mobile devices	MDM agent	The MDM agent permits download of campus data from its official email domain only and only allow upload and sending of data to the official email domain only. After a specified duration of time the downloaded data on the device is wiped out by the agent. Download of campus data from its accessible servers is permitted but wiped out after the specified period expires. The agent permits upload and sending of data from the server to official email domain only. The agent protects the campus data the device holds from access by another device before it wipes it out.

Table 3: BYOD security Challenges that KANYI BYOD Security framework will address.

CHAPTER FOUR

DESIGN OF THE NETWORK MODEL, SIMULATION AND DISCUSSION

4.1 Introduction

KANYI BYOD framework that is described and illustrated in chapter 3 above was designed into a network topology in order to integrate the BYOD model to the campus network. The BYOD network topology was evaluated using OPNET modeler for security vulnerability. The BYOD network topology model that implements the KANYI BYOD security model is as shown in Figure 4.

4.2 Proposed Network Topology to Integrate Kanyi BYOD Framework to the Campus Network

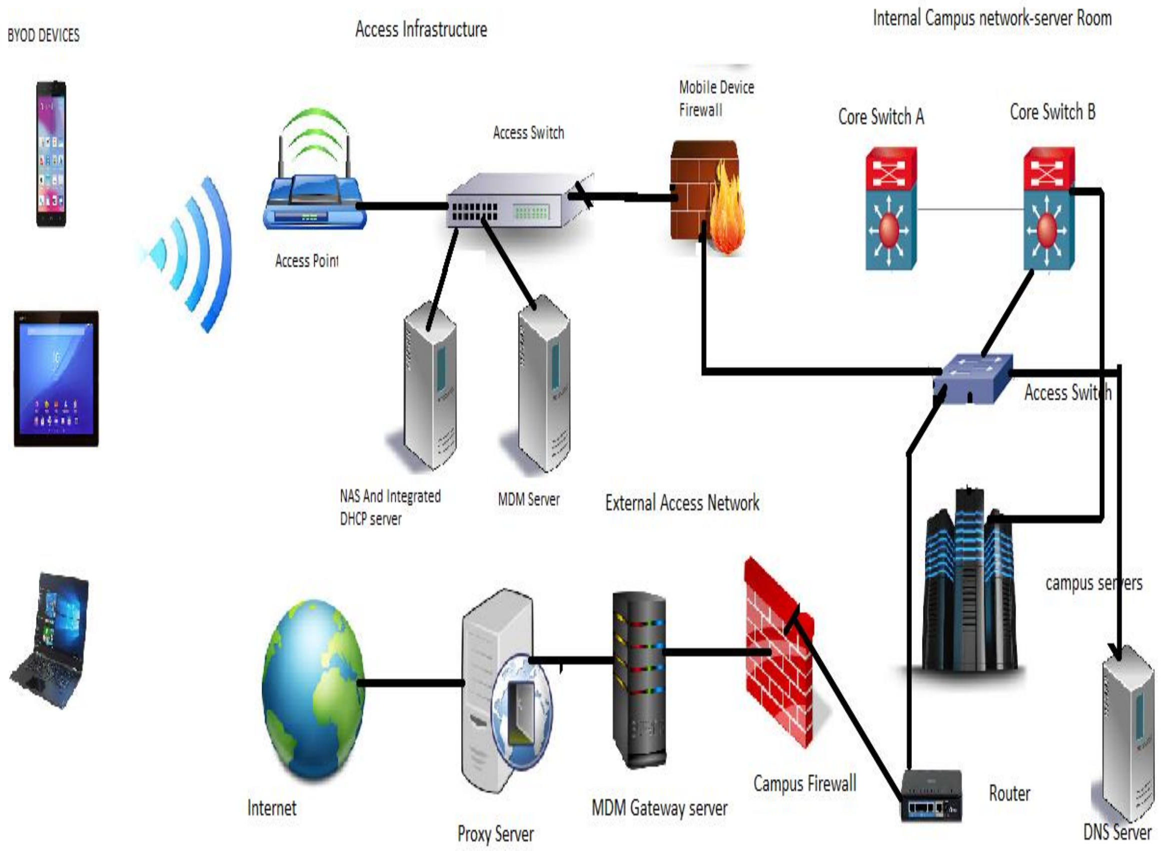


Figure 4: Proposed network Topology to integrate KANYI BYOD Security framework to the Campus network.

As illustrated in figure 4 above the network topology of campus network environment comprising of mobile devices. The model will be tested using simulation methodology for security vulnerability.

The topology comprises of the following entities:

- Terminal devices- mobile devices such as tablet, smartphone and laptop and applications running in the mobile devices

- The Access network: Access point, access switch, NAS server, MDM server and Mobile device Firewall are part of the connection network.
- Campus network- this is the university network found in the server room comprising of switches, router, firewall, servers and proxy server. The campus network is regarded as the internal network in this model where university systems are hosted. The campus network should be protected from threats brought about by mobile devices.
- External network access- This zone comprises of security devices- Campus Firewall, MDM gateway server and Proxy server that ensure safe exit of traffic from the campus network to the internet and safe entry back.

The BYOD network topology is broken down into domains as follows:

- Domain 1: Terminal devices- This domain will tackle the mobile operating system, device type and installed applications. The scanning of the terminal devices in order to determine the above and their vulnerabilities is the responsibility of the MDM agent installed by the MDM server to the device.
- Domain 2: Access Network- This domain will tackle secure access of a mobile device to the campus network. Secure access is guaranteed by the MDM agent, NAS server and Mobile device Firewall.
- Domain 3: Campus network- this domain will tackle the internal servers hosting campus systems and services. Campus network can be referred to as the server room. The campus network comprises of servers, core switches, switches, and a router.
- Domain 4: External Network access- this domain will tackle the security of campus network from the internet activities of mobile devices. External network access comprises of campus firewall, MDM gateway server and proxy server.

4.3 Security Threats Evaluations by Attack Scenarios

The framework was subjected to various attacker scenarios. In this section results from the various security threats evaluations obtained from attack scenarios on the proposed network model in mobile computing environments will be shown. Based on the above specified domains attacks can be classified as either outside or inside attacks. In both attack types the target of the attack is the campus network hosting the servers or another Mobile device.

In the case of the outsider attack the attacker installs a malware on a mobile device that is already granted access and has internet connectivity. The attacker will therefore move from domain 4 to domain 1 then proceed to domain 3 which is the target of attack through domain 2.

In the second Case the outside attacker will move from domain 4 to domain 1 where the target device is located through domain 2. An insider attacker is any legitimate mobile device owner that is connected to the campus network and wishes to attack the campus network. The attack path starts from domain1 to domain 3 through domain 2.

In the second case the inside attacker will attack from domain 1 where the attack device is located then proceed to domain 2 in order to attack the device located in domain 1 again. The figure 9 below shows a graph that represents the attack paths through the proposed network model that is based on mobile computing and networking environment. This helps to illustrate the attack paths through the model and therefore make it easier to grasp the attack paths.

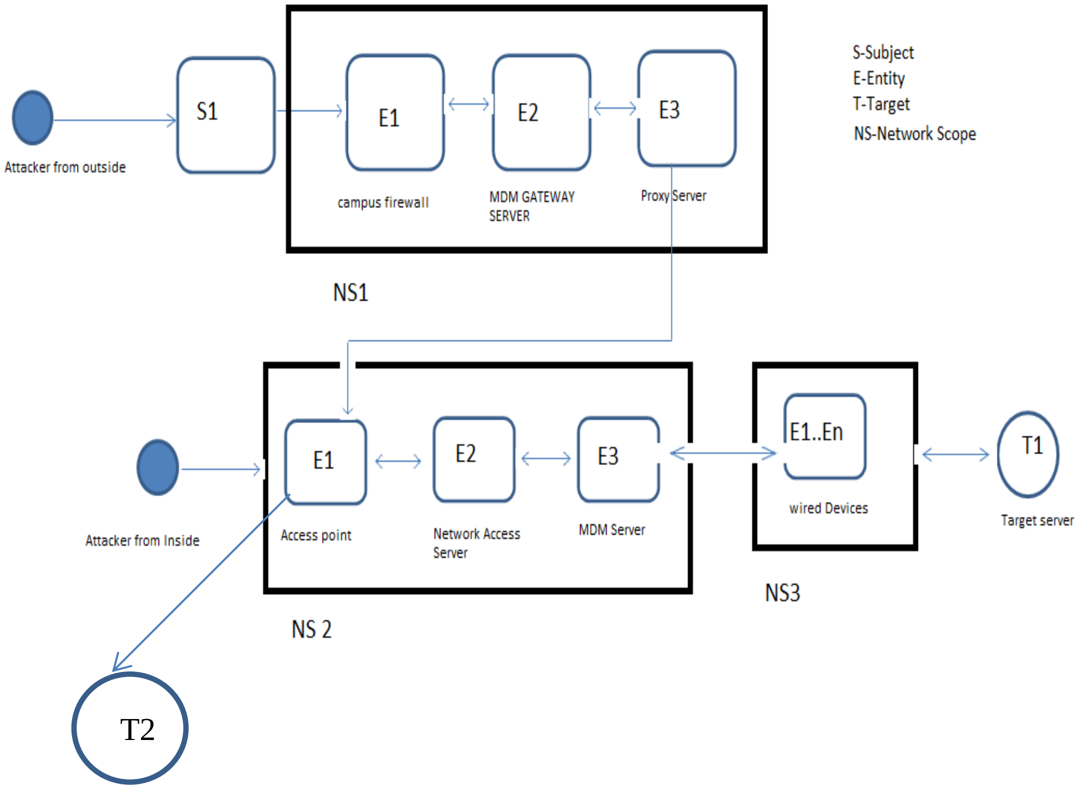


Figure 5: A graph of the Attack paths through the proposed framework

From the graph above there are two attack paths to the target which is a server in the campus network from the mobile device which is the source of the attack.

Based on the graph S1 is the subject in this case the mobile computing device used to attack target T1-enterprise server, E= (E1, E2,…En) are the networking equipment used to implement the model and NS comprises of all entities E1, E2,..En.

The attack paths are highlighted as below:

The outside attack is initiated from Domain 4:

Case 1:

S1 → NS1{E1 → E2 → E3} → NS2{E1 → E2 → E3} → NS3{E1..En} → T1

Case 2:

S1 → NS1{E1 → E2 → E3} → NS2{E1} → T2

The Inside attack is initiated from Domain 1:

Case 3:

S1 → NS2{E1 → E2 → E3 → E4} → NS3{E1..En} → T1

Case 4:

S1 → NS2{E1} → T2

4.3.1 Quantification for Security Vulnerability Associated With the Proposed Framework

Based on the above cases there are several methods to calculate the quantification for security vulnerability associated with the proposed model. The security threats evaluation performance of the proposed network model (implementation of the BYOD model) will be based on CVSS (Common Vulnerability Scoring System) Version 2 method which provides an open framework for communicating the characteristics and impact of ICT vulnerabilities. Based on the CVSS version 2 the following Base Metrics will be considered:

- **Access Vector (AV)**: determines whether the vulnerability is exploitable locally or remotely.

Value	Description	Score
Local(L)	The attacker must either have physical access to the vulnerable system (e.g. firewire attacks) or a local account (e.g. a privilege escalation attack).	0.395
Adjacent Network (A)	The attacker must have access to the broadcast or collision domain of the vulnerable system (e.g. ARP spoofing, Bluetooth attacks).	0.646
Network (N)	The vulnerable interface is working at layer 3 or above of the OSI Network stack. These types of vulnerabilities are often described as remotely exploitable (e.g. a remote buffer	1.0

	overflow in a network service)	

Table 4: Access Vector metric details

- **Access Complexity (AC):** this is the complexity of the attack needed to exploit the vulnerability once an attacker has access to the target system.

Value	Description	Score
High (H)	Specialized conditions exist, such as a race condition with a narrow window, or a requirement for social engineering methods that would be readily noticed by knowledgeable people.	0.35
Medium (M)	There are some additional requirements for access, such as a limit on the origin of the attacks, or a requirement for the vulnerable system to be running with an uncommon, non-default configuration.	0.61
Low (L)	There are no special conditions for access to the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.	0.71

Table 5: Access Complexity metric details

- **Authentication (Au):** whether an attacker requires to be authenticated to the target system in order to exploit the vulnerability.

Value	Description	Score
Multiple (M)	Exploitation of the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time.	0.45
Single (S)	The attacker must authenticate once in order to exploit the vulnerability.	0.56
None (N)	There is no requirement for the attacker to authenticate.	0.704

Table 6: Authentication metric details

The following Impact metrics will be considered:

- **Confidentiality (C):** this metric describes the impact on the confidentiality of data processed by the system.

Value	Description	Score
None (N)	There is no impact on the confidentiality of the system.	0.0
Partial (P)	There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available.	0.275
Complete (C)	There is total information disclosure, providing access to any / all data on the system.	0.660

Table 7: Confidentiality impact metric details

- **Integrity (I):** this metric describes the impact on the integrity of the exploited system.

Value	Description	Score
None (N)	There is no impact on the confidentiality of the system.	0.0
Partial (P)	Modification of some data or system files is possible, but the scope of the modification is limited.	0.275
Complete (C)	There is total loss of integrity; the attacker can modify any files or information on the target system.	0.660

Table 8: Integrity impact metric details

- **Availability (A):** metric describes the impact on the integrity of the exploited system.

Value	Description	Score
None (N)	There is no impact on the confidentiality of the system.	0.0
Partial (P)	There is reduced performance or loss of some functionality.	0.275
Complete (C)	There is total loss of availability of the attacked resource.	0.660

Table 9: Availability impact metric details

The above metrics are concatenated to produce the CVSS Vector for the vulnerability.

These six metrics are used to calculate the exploitability and impact sub-scores of the vulnerability. These sub-scores are used to calculate the overall base score.

Calculations:

Exploitability=20 X Access Vector X Access Complexity X Authentication

Impact= 10.41 X (1-(1-ConfImpact) X (1-InteImpact) X (1-AvailImpact))

$$f(impact = \begin{cases} 0, & \text{if Impact = 0} \\ 1.176, & \text{otherwise} \end{cases}$$

BaseScore = roundto1Decimal ((0.6 X Impact) + (0.4 X Exploitability) – 1.5) X f(impact))

The base vectors of the above cases will be calculated based on CVSS version 2.

Case 1: The attacker has to gain entry into the mobile device (laptop-due to its computing capability) first through the external network comprised of Campus firewall, MDM gateway server and proxy server to the access point in order to use the mobile device as subject of attack. **AV** is therefore set to Network (N) because it is possible to access far in the distance via the internet. **AC** is set to Medium (M) because the attacker would need socio technological method to access the target system. **Au** is set to Single (S) since to access the targeted interior campus system log in using password, single-sign-on and certificates is needed. If this interior campus system is infected with a malware it may be almost entirely exposed to danger. Each of the impact values(C, I and A) would therefore be set to Complete (C) in order to consider and work with the most dangerous case scenario. The base sector of this vulnerability would thus be represented as: AV:*N*/AC:*M*/Au:*S*/C:*C*/I:*C*/A:*C*. A base Score of this case is calculated by a temporal score including the vulnerability values and a result of 8.5 is gotten as shown in the table 10.

Case 2: The attacker has to gain entry into target mobile device (tablet and smartphones) through the external network comprised of Campus firewall, MDM gateway server and proxy server to the access point in order to gain access to the target mobile device. **AV** is therefore set to Network (N) because it is possible to access far in the distance via the internet. **AC** is set to Medium (M) because the attacker would need some expertise to crack the firewall, MDM gateway server and Proxy server in order to gain access through the access point. **Au** is set to None (N) since the mobile device is already authenticated and connected through the Access point and therefore the attacker does not need to be authenticated. For the C impact it is set to Complete (C) while I and A are set to Partial (P) because smart phones and tablets have a restricted access and performance. The base sector of this vulnerability would thus be represented as: AV:*N*/AC:*M*/Au:*N*/C:*C*/I:*P*/A:*P*. A base Score of this case is calculated by a temporal score including the vulnerability values and a result of 8.3 is gotten as shown in the table 10.

Case 3: The attacker in this case is an insider who is authenticated and connected to the campus network and has an intention of launching an attack on the interior campus system. **AV** is therefore set to Adjacent Network (A) because the attacker is in front of the campus firewall, MDM gateway server and Proxy server and is indeed within NS2 as shown in figure 5. **AC** is set to Low (L) because the attacker has a better command for penetration into the interior campus systems. **Au** is set to Single (S) since to access the targeted interior campus system log in using password, single-sign-on and certificates is needed. Similar to Case 1 each of the impact values(C, I and A) would therefore be set to Complete (C) in order to consider and work with the most dangerous case scenario. The base sector of this vulnerability would thus be represented as: AV:*A*/AC:*L/*Au:*S*/C:*C*/I:*C*/A:*C.* A base Score of this case is calculated by a temporal score including the vulnerability values and a result of 7.7 is gotten as shown in the table 10.

Case 4: The attacker in this case is an insider who is authenticated and connected to the campus network and has an intention of launching an attack on another mobile device that is authenticated and connected. **AV** is therefore set to Adjacent Network (A) because the attacker is in front of the campus firewall, MDM gateway server and Proxy server and is indeed within NS2 as shown in figure 7. **AC** is set to Low (L) because the attacker has a better command for penetration into the mobile device through the access point. **Au** is set to None (N) since both devices are authenticated and connected and therefore no other authentication is needed. For the C impact it is set to Complete (C) while I and A are set to Partial (P) because smart phones and tablets have a restricted access and performance. The base sector of this vulnerability would thus be represented as: AV:*A*/AC:*L/*Au:*N*/C:*C*/I:*P*/A:*P.* A base Score of this case is calculated by a temporal score including the vulnerability values and a result of 7.3 is gotten as shown in the table 10.

CVSS Metrics	**Case 1**	**Case 2**	**Case 3**	**Case 4**
Access Vector(AV)	N:1.0	N: 1.0	A: 0.646	A: 0.646
Access Complexity (AV)	M: 0.61	M: 0.61	L: 0.71	L: 0.71
Authentication (Au)	S: 0.56	N: 0.704	S: 0.56	N: 0.704
Confidentiality Impact(C)	C: 0.66	C: 0.66	C: 0.66	C: 0.66
Integrity Impact (I)	C: 0.66	P: 0.275	C: 0.66	P: 0.275
Availability Impact(A)	C: 0.66	P: 0.275	C: 0.66	P: 0.275
Base Score	8.5	8.3	7.7	7.3

Table 10: Analysis of the Four Cases.

From the above table it is clear that the four cases have vulnerabilities that are ranked as High severity. The highest priority in terms of security should therefore be assigned to Case 1 and 2 which represent outside attack.

4.4 Simulation for Security Vulnerability Test

4.4.1 Opnet Network Setup

The proposed BYOD network model was setup using Opnet simulator version 14.5. The figure below is a screen shot of the designed model on the simulator.

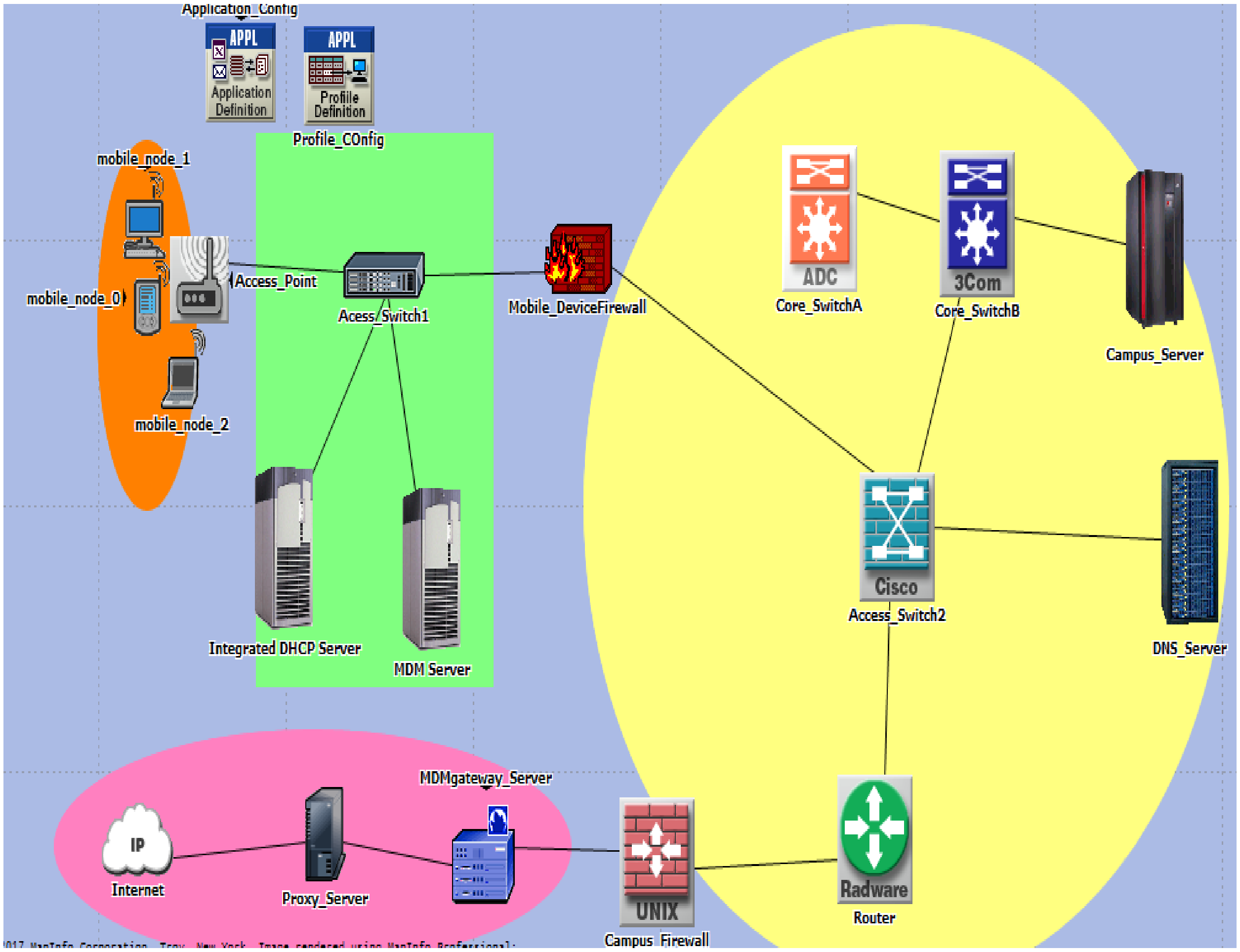
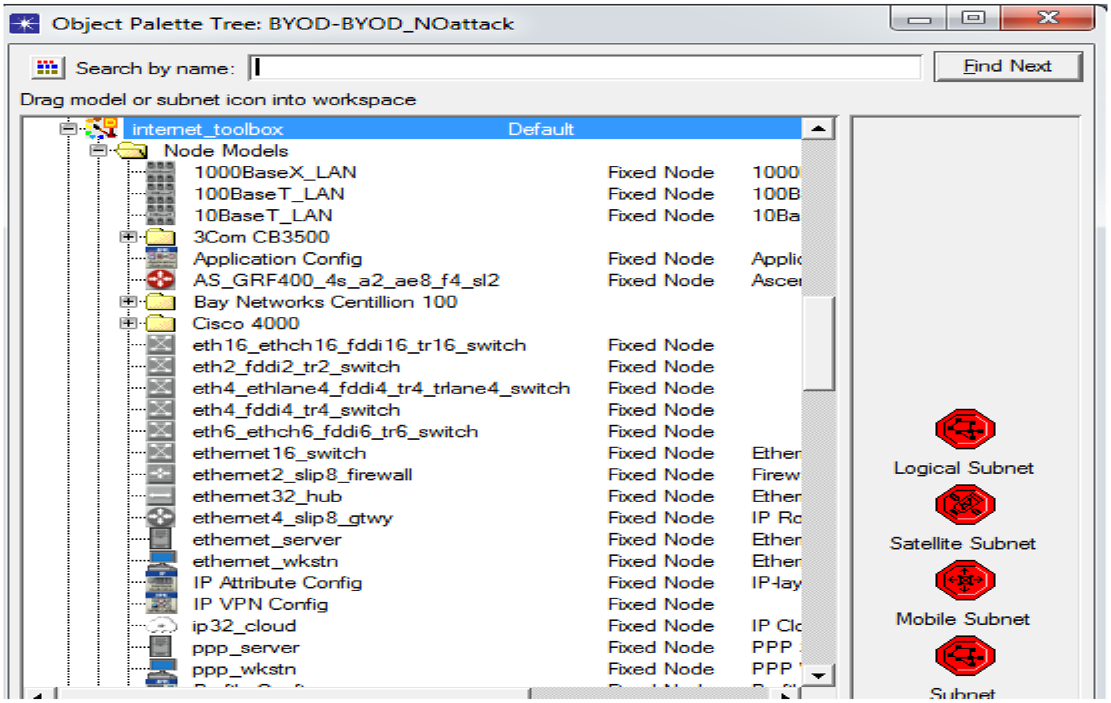


Figure 6: Screen Shot of KANYI BYOD network model design in Opnet Simulator.

The BYOD devices are marked in orange circle, the core campus network is shown in yellow circle and the external network is shown in pink circle. In order to configure the network, all the key components such as BYOD workstation, BYOD mobile devices,Access point, Access switch and Core switch, Router and firewall, and different kind of servers are selected from the object palatte which is shown in figure 7.



Object Palette Tree: BYOD-BYOD_NOattack

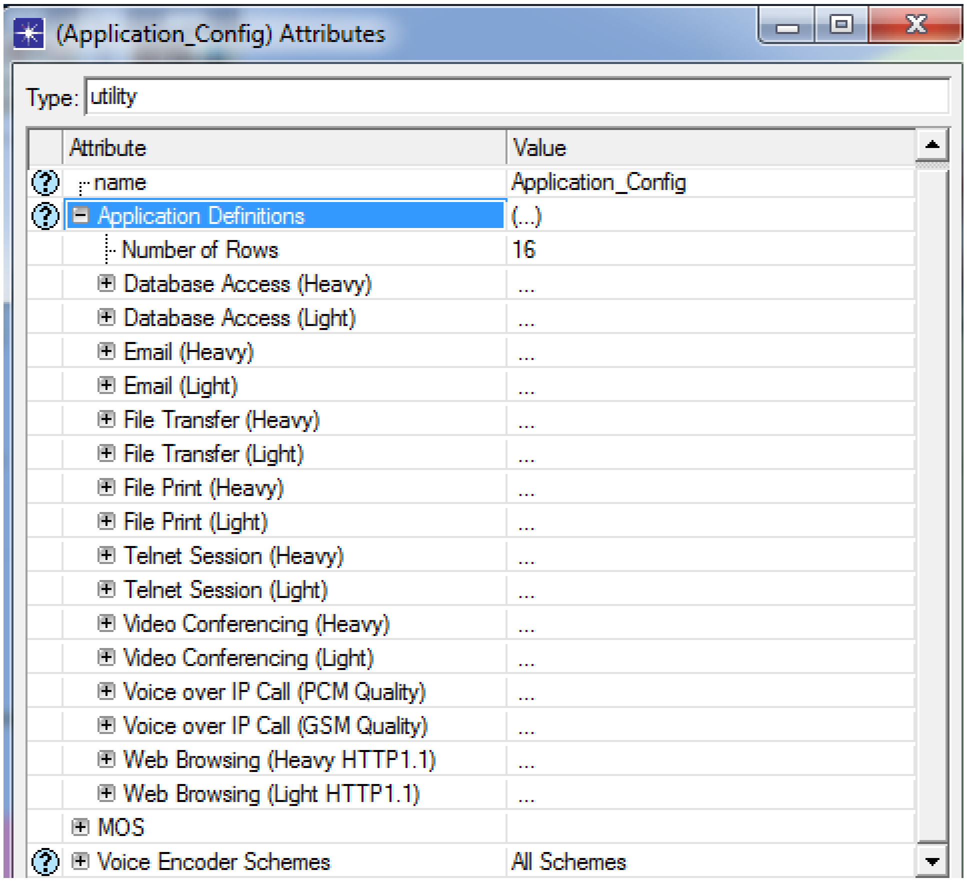
Search by name:

Drag model or subnet icon into workspace

```
internet_toolbox                              Default
  Node Models
    1000BaseX_LAN                             Fixed Node   1000
    100BaseT_LAN                              Fixed Node   100B
    10BaseT_LAN                               Fixed Node   10Ba
    3Com CB3500
    Application Config                        Fixed Node   Applic
    AS_GRF400_4s_a2_ae8_f4_sl2                Fixed Node   Ascer
    Bay Networks Centillion 100
    Cisco 4000
    eth16_ethch16_fddi16_tr16_switch          Fixed Node
    eth2_fddi2_tr2_switch                     Fixed Node
    eth4_ethlane4_fddi4_tr4_trlane4_switch    Fixed Node
    eth4_fddi4_tr4_switch                     Fixed Node
    eth6_ethch6_fddi6_tr6_switch              Fixed Node
    ethernet16_switch                         Fixed Node   Ether
    ethernet2_slip8_firewall                  Fixed Node   Firew
    ethernet32_hub                            Fixed Node   Ether
    ethernet4_slip8_gtwy                      Fixed Node   IP Ro
    ethernet_server                           Fixed Node   Ether
    ethernet_wkstn                            Fixed Node   Ether
    IP Attribute Config                       Fixed Node   IP-lay
    IP VPN Config                             Fixed Node
    ip32_cloud                                Fixed Node   IP Clo
    ppp_server                                Fixed Node   PPP
    ppp_wkstn                                 Fixed Node   PPP
```

Figure 7: Screen Shot of Opnet Simulator Objects Palette tree

In order to set up traffic among nodes located in different locations in this model, various applications like File Transfer (FTP), Http, database are set up from OPNET application configuration attribute which is shown in Figure 8.



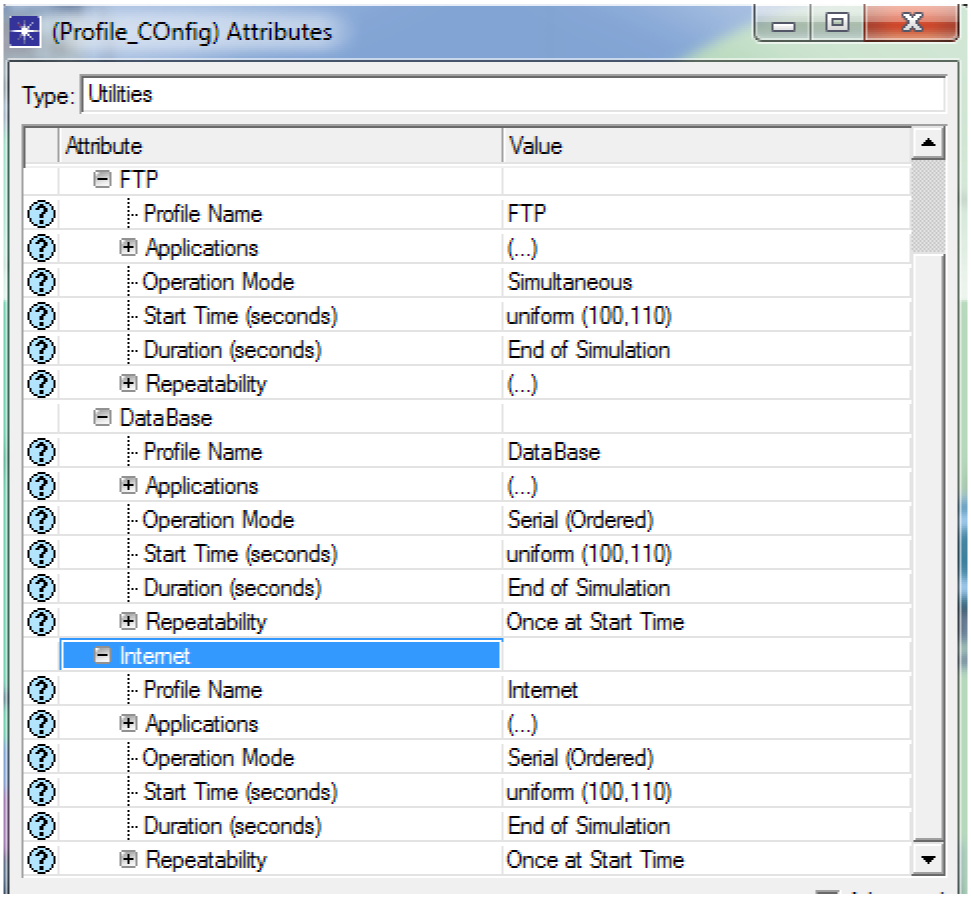
(Application_Config) Attributes

Type: utility

Attribute	Value
name	Application_Config
⊟ Application Definitions	(...)
Number of Rows	16
⊞ Database Access (Heavy)	...
⊞ Database Access (Light)	...
⊞ Email (Heavy)	...
⊞ Email (Light)	...
⊞ File Transfer (Heavy)	...
⊞ File Transfer (Light)	...
⊞ File Print (Heavy)	...
⊞ File Print (Light)	...
⊞ Telnet Session (Heavy)	...
⊞ Telnet Session (Light)	...
⊞ Video Conferencing (Heavy)	...
⊞ Video Conferencing (Light)	...
⊞ Voice over IP Call (PCM Quality)	...
⊞ Voice over IP Call (GSM Quality)	...
⊞ Web Browsing (Heavy HTTP1.1)	...
⊞ Web Browsing (Light HTTP1.1)	...
⊞ MOS	
⊞ Voice Encoder Schemes	All Schemes

Figure 8: Screen Shot of OPNET application configuration attribute

Each of the applications configured as shown in figure 10 requires exclusive user profile to operate from one point to another point of the network. The profile configuration attribute is used is as captured by Figure 9.



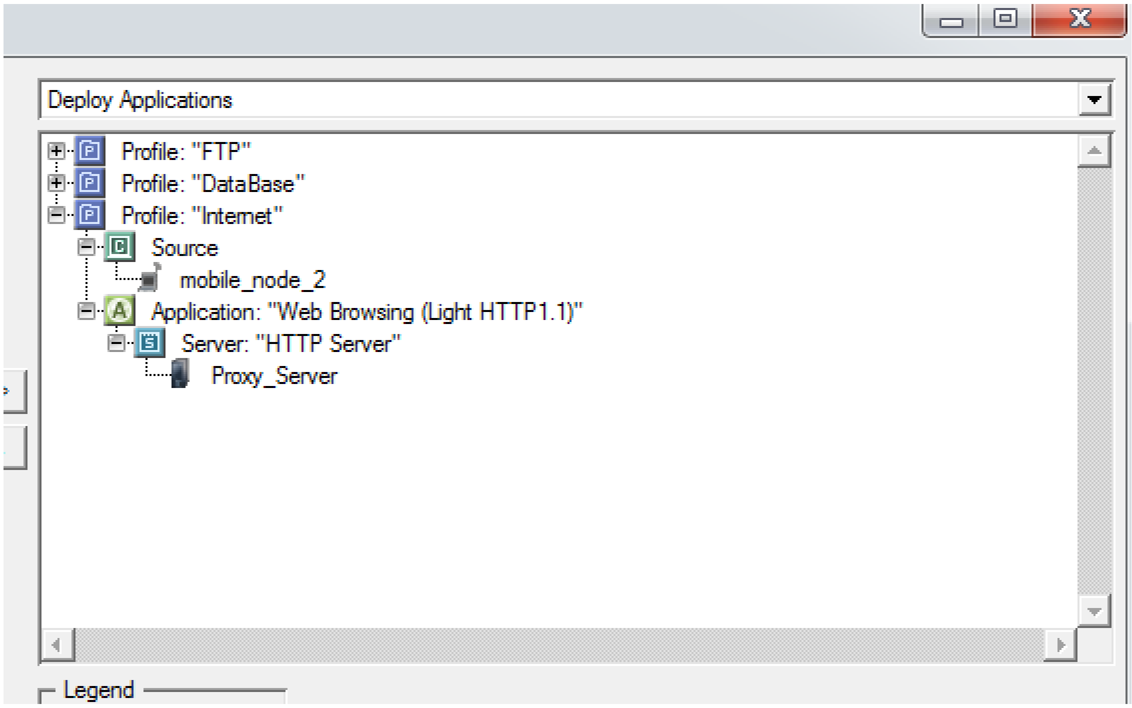
(Profile_COnfig) Attributes

Type: Utilities

Attribute	Value
⊟ FTP	
Profile Name	FTP
⊞ Applications	(...)
Operation Mode	Simultaneous
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	(...)
⊟ DataBase	
Profile Name	DataBase
⊞ Applications	(...)
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time
⊟ Internet	
Profile Name	Internet
⊞ Applications	(...)
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time

Figure 9: Screen Shot of OPNET Profile configuration attribute

After configuring all the applications and required profile configuration, next activity is the set up of traffic between set of source and destination nodes as illustrated in Figure 10. It can be seen that mobile_node_2 is configured to send http request to the proxy server for browsing internet. In a similar fashion all network nodes also take part in FTP and database application data exchange.



Deploy Applications

```
Profile: "FTP"
Profile: "DataBase"
Profile: "Internet"
    Source
        mobile_node_2
    Application: "Web Browsing (Light HTTP1.1)"
        Server: "HTTP Server"
            Proxy_Server
```

Figure 10: Screen shot of deployment of Applications

Three scenario are created for the purpose of comparing the simulation results:

- Scenario 1- BYOD Simulation with no attack
- Scenario 2- BYOD simulation with an attacker mobile node
- Scenario 3-BYOD simulation with Preventive measurers in place.

4.5 BYOD Network Attack Simulation

KANYI BYOD network model was subjected to an attacker launching ping flood attack as shown in Figure 11. The attacker was targetting campus server with very large ping packet creating a huge congestion all over the network.

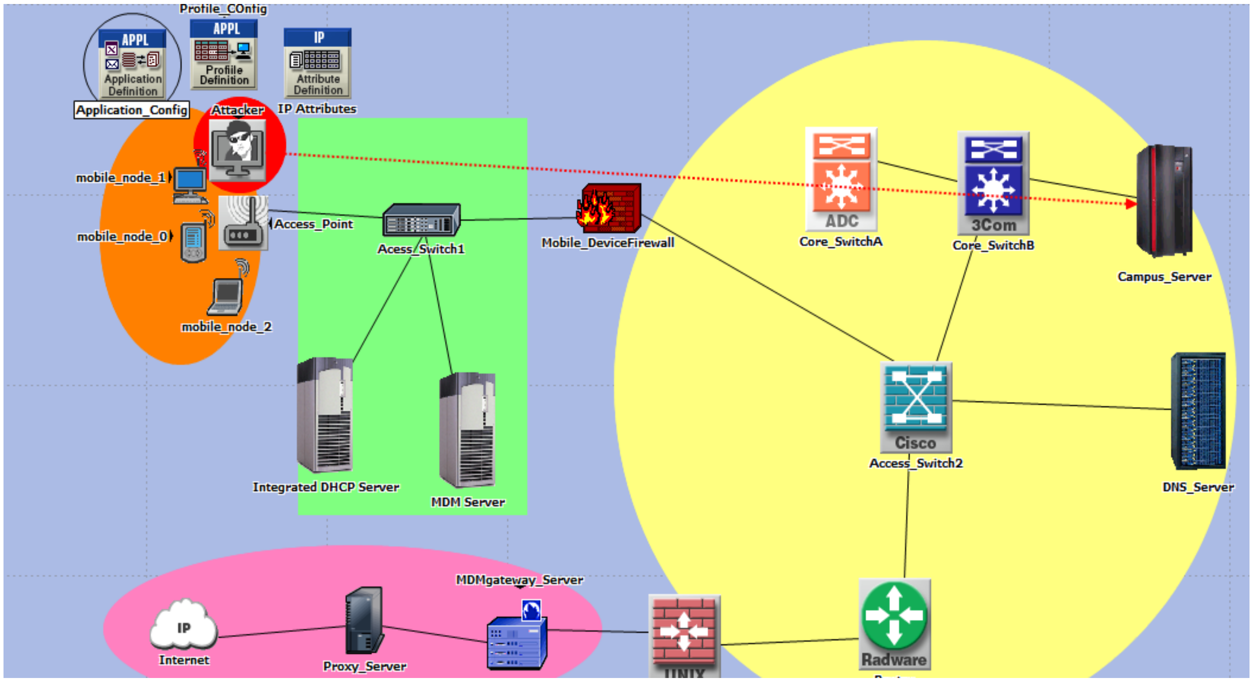
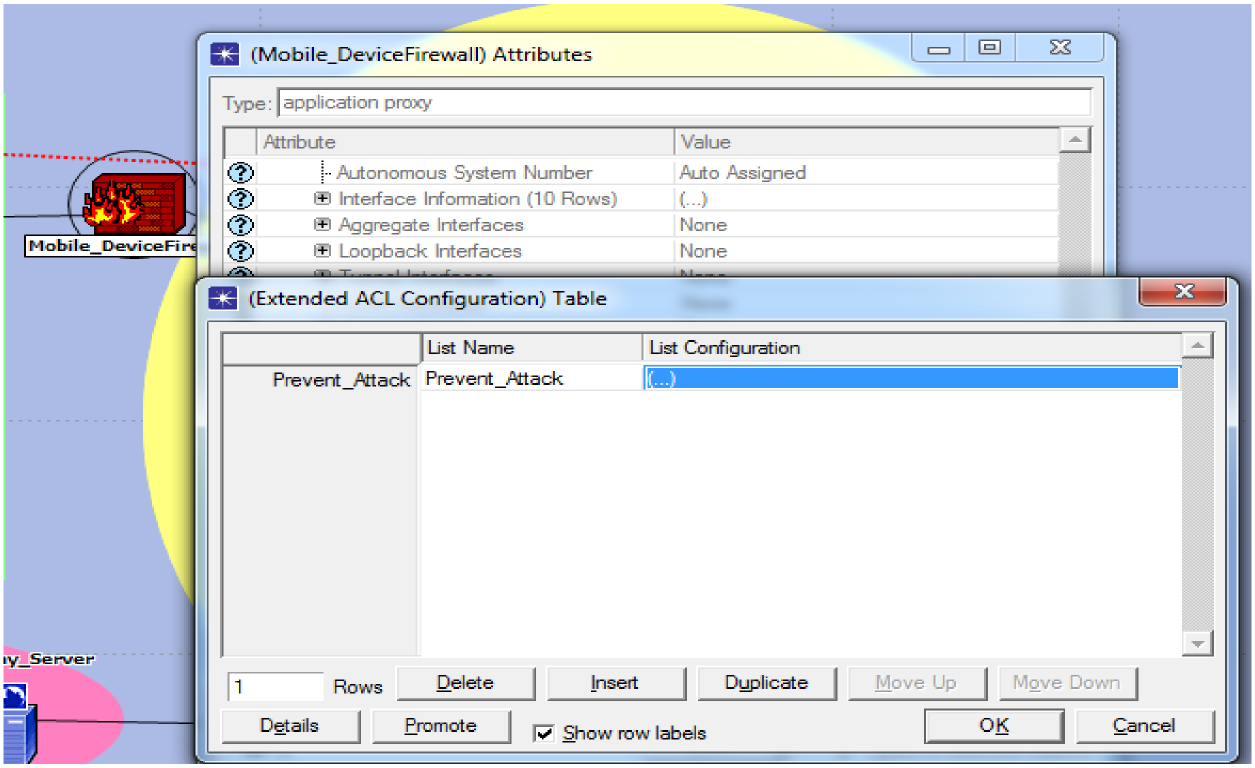


Figure 11: Screen shot of an attacker mobile node targeting the campus server

4.6 BYOD Attack Prevention

Considering the attacker's presence in the already running BYOD network , some steps were taken to prevent the attack –Scenario 3. The campus network has got an incoming firewall known as mobile device firewall, in which an access control list is configured as shown in the figure 12 in order to stop ICMP attack from the attacker mobile node.



(Mobile_DeviceFirewall) Attributes

Type: application proxy

Attribute	Value
Autonomous System Number	Auto Assigned
⊞ Interface Information (10 Rows)	(...)
⊞ Aggregate Interfaces	None
⊞ Loopback Interfaces	None

(Extended ACL Configuration) Table

	List Name	List Configuration
Prevent_Attack	Prevent_Attack	(...)

1 Rows

Figure 12: Screen shot of Mobile device Firewall ACL configuration

4.7 Comparison of the Three Scenarios

Simulation for the three scenarios was done and the screen shots of resulting graphs of the simulation are as shown below.

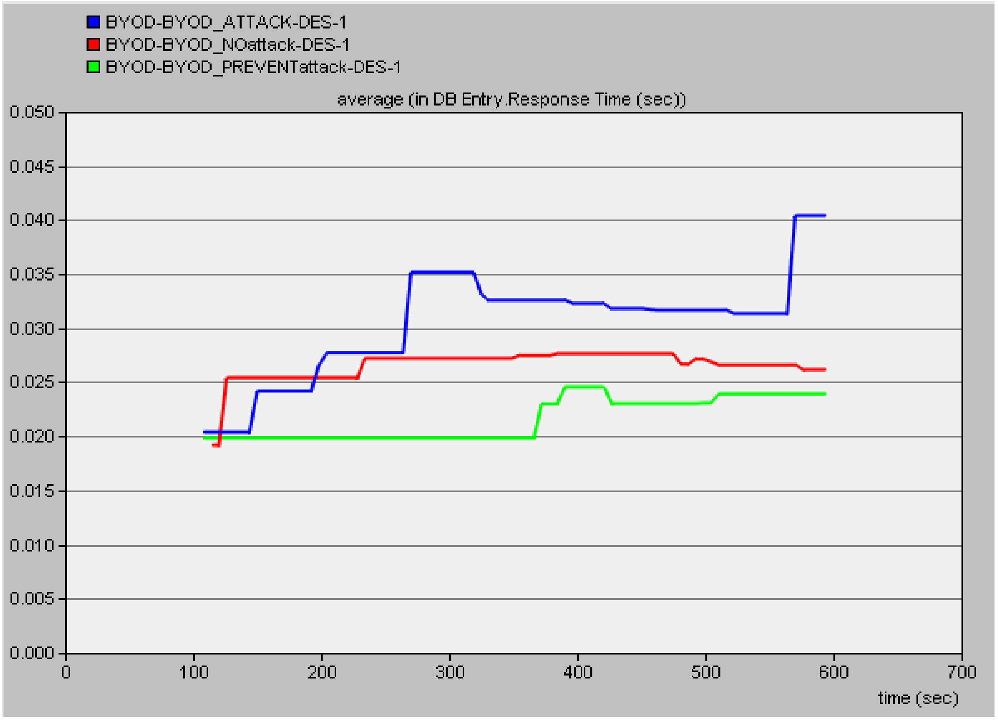


Figure 13: Screen shot of simulation results of the three scenarios in relation to the Database application(entry) of the target server.

When there is not attack in the BYOD network the response rate of the database application (entry application) to the request made by the mobile_node 2 is less as compared to when there is an attacker scenario. When preventive measurers are put in place the database application response rate reduces to normal rates.

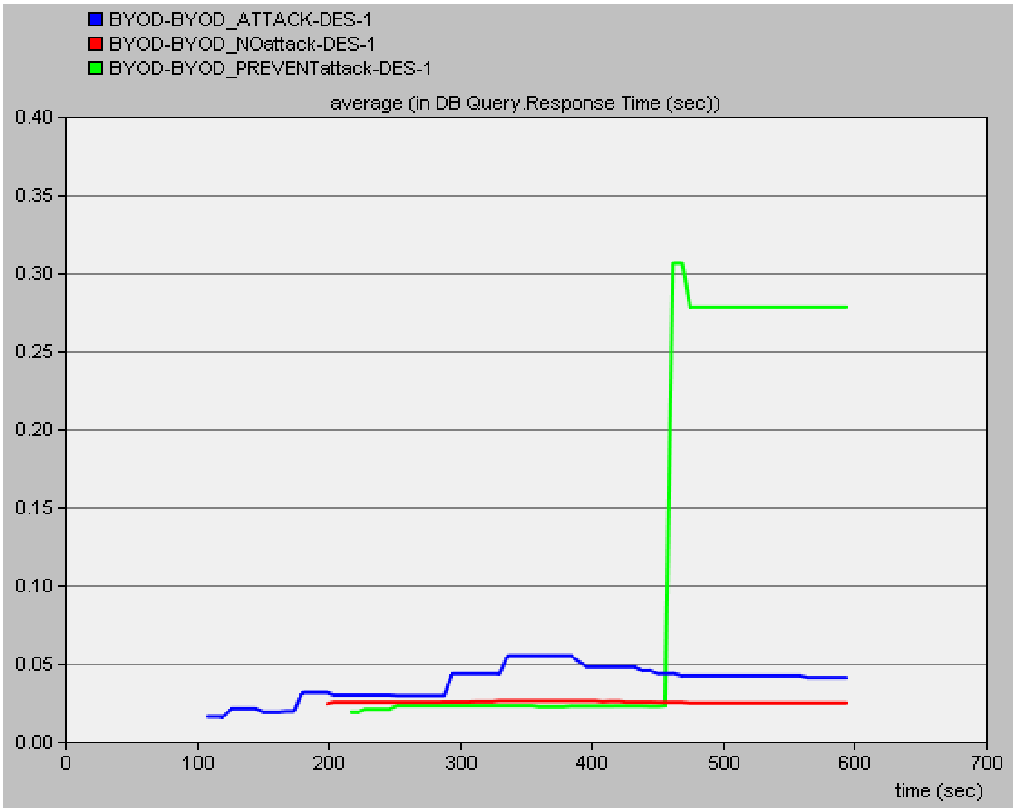


Figure 14: Screen shot of simulation results of the three scenarios in relation to the Database application(query) of the target server.

When there is no attack in the BYOD network the response rate of the database application (query) to the request made by the mobile_node 2 is less as compared to when there is an attacker scenario. When preventive measurers are put in place, the database application response rate reduces to normal rates based on the entire traffic from all connected devices .

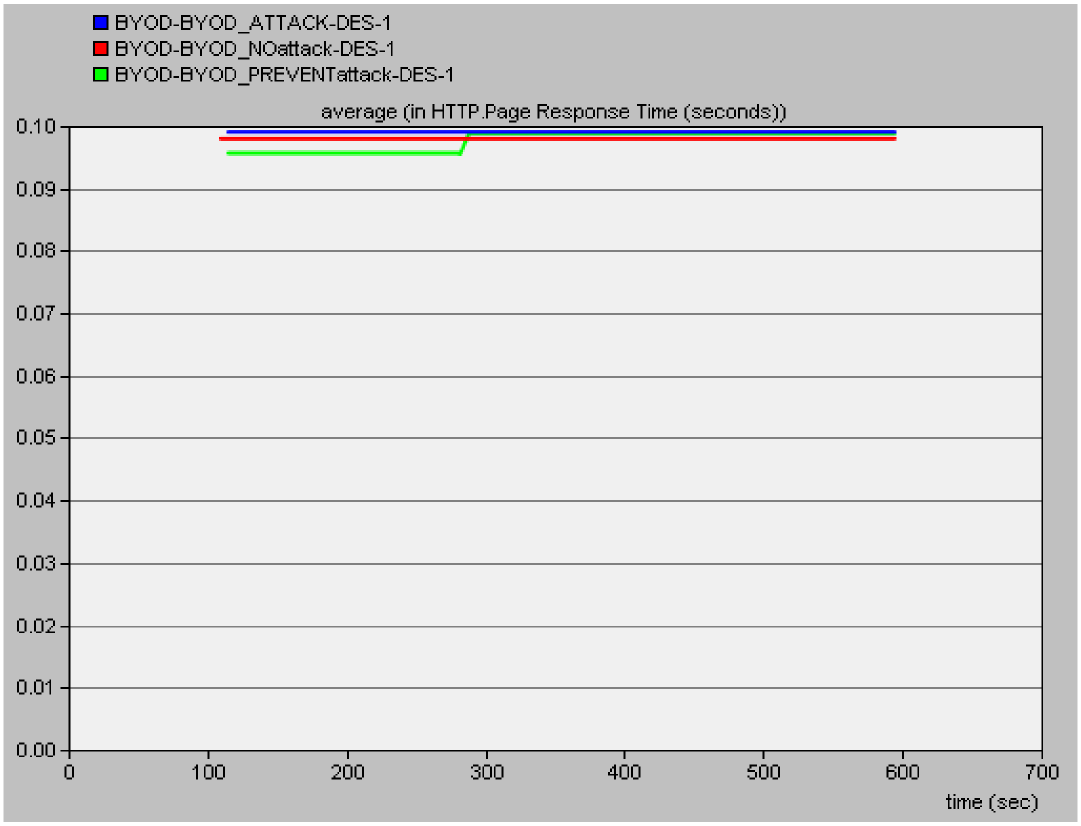


Figure 15: Screen shot of simulation results of the three scenarios in relation to the HTTP(web service) application of the target server.

When there is no attack in the BYOD network, the response rate of the HTTP application from the target server to the request made by the mobile_node 2 is less as compared to when there is an attacker scenario. When preventive measurers are put in place the HTTP application response rate reduces to normal rates based on the number of mobile devices in connection.

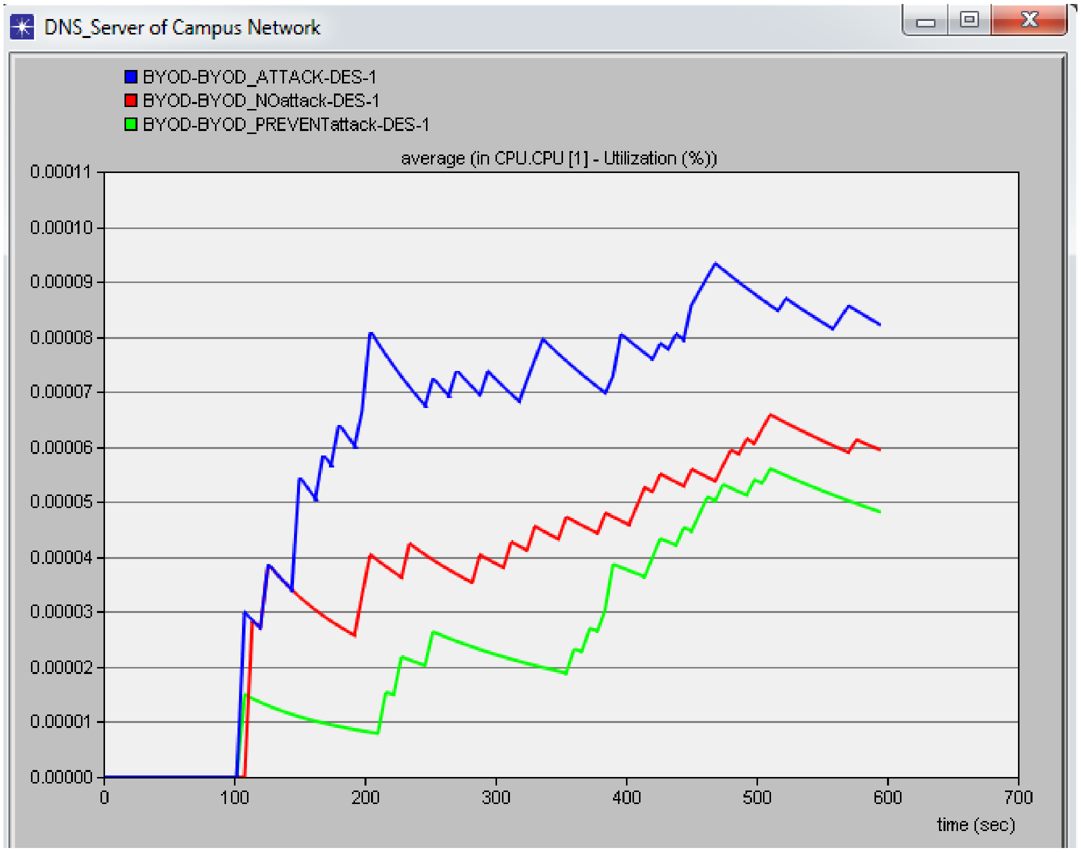


Figure 16: Screen shot of simulation results of the three scenarios in relation to the DNS server CPU performance.

When there is no attack in the BYOD network, CPU performance is less as when there is an attacker scenario. When preventive measurers are put in place the CPU performance of the DNS server goes to normal rates.

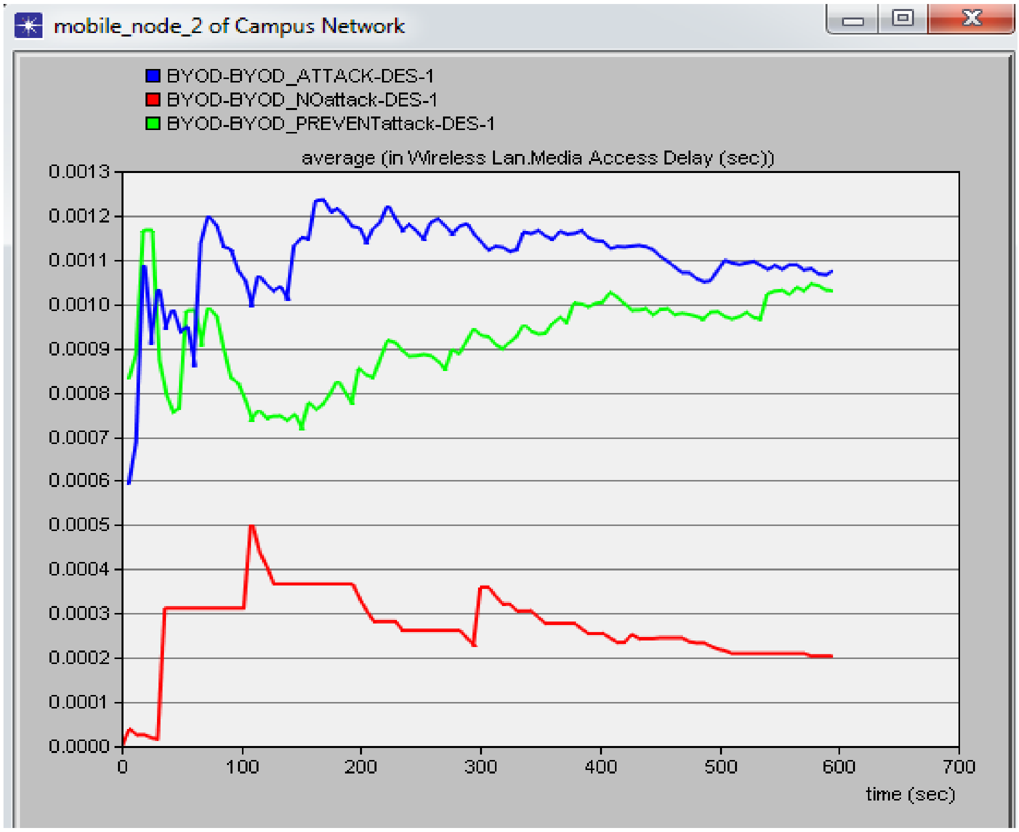


Figure 17: Screen shot of simulation results of the three scenarios in relation to mobile_ node 2 WLAN media access delay.

When there is no attack in the BYOD network, WLAN media access delay of the mobile_node 2 is much less as when there is an attacker scenario. When preventive measurers are put in place the WLAN media access delay of the node is reduced but is higher as compared to no BYOD attack due to access control brought about by the Mobile devices firewall.

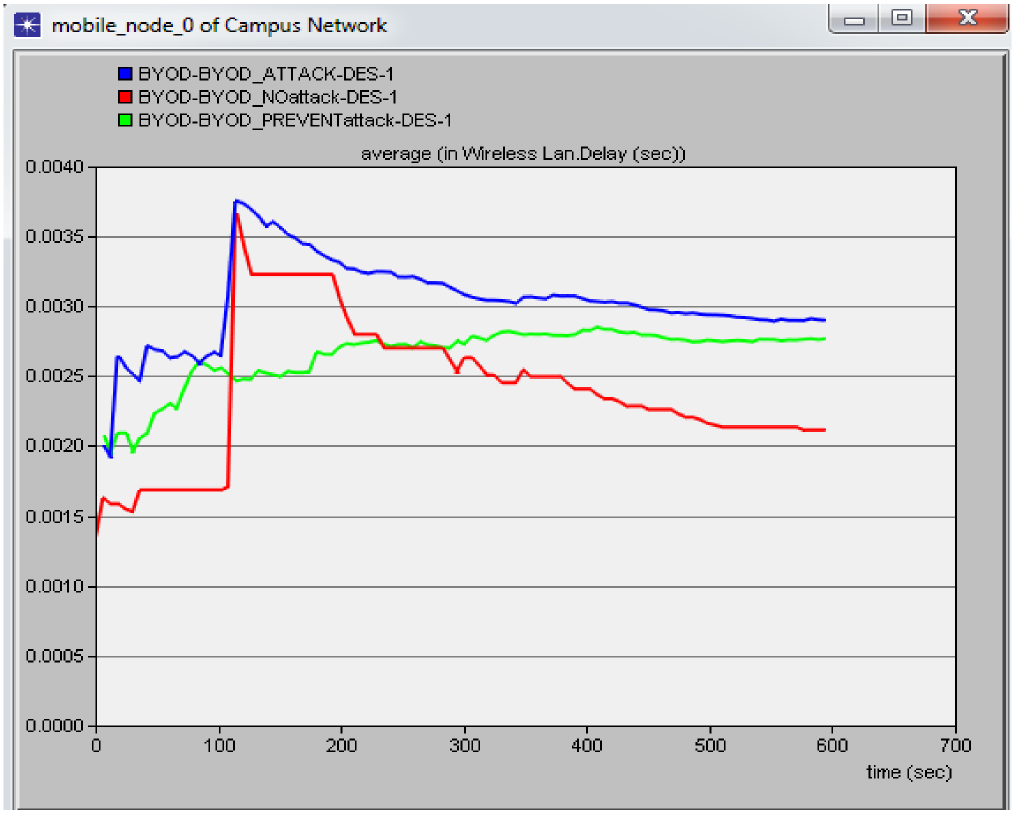


Figure 18: Screen shot of simulation results of the three scenarios in relation to mobile_ node 0 WLAN delay.

When there is no attack in the BYOD network, WLAN delay (performance of the WLAN) as measured from the mobile_node 0 is better as compared to when there is an attacker scenario. When preventive measurers are put in place the WLAN delay is reduced but is higher as compared to no BYOD attack due to access control brought about by the Mobile devices firewall.

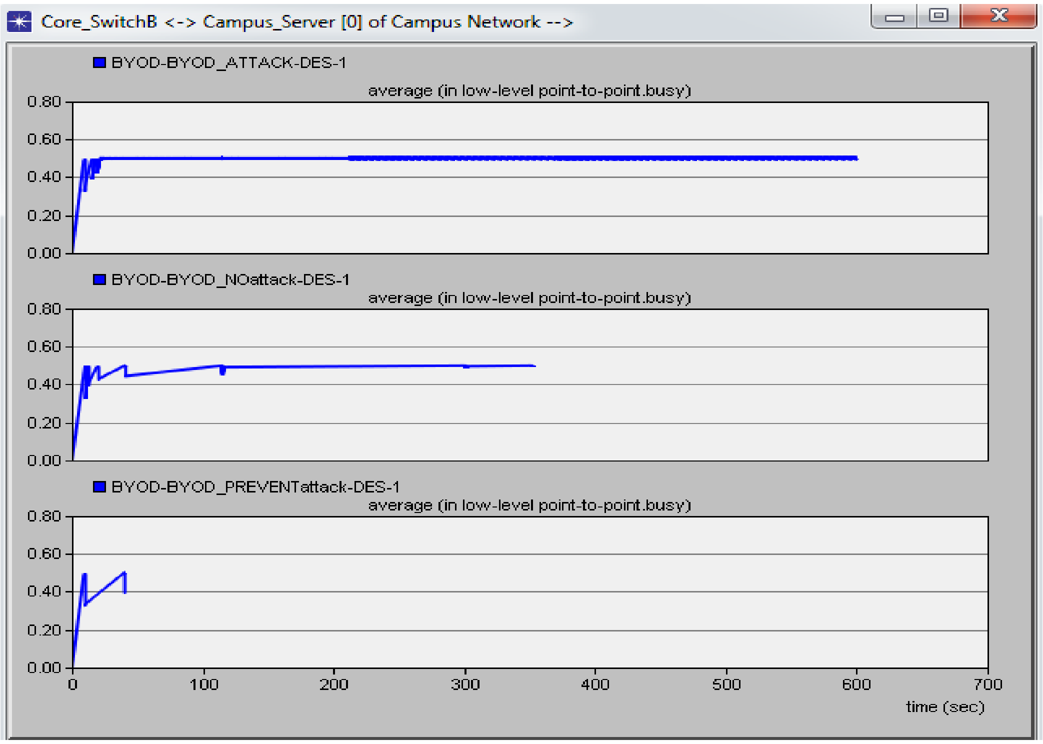


Figure 19: Screen shot of simulation results of the three scenarios in relation to Core Switch B traffic flow to and from Campus server

When there is no attack in the BYOD network, the network traffic between Core Switch B and Campus Server is less as compared to when there is an attacker scenario. When preventive measurers are put in place the network traffic reduces further due to less traffic going through the Core Switch B to the campus server from mobile devices.

4.8 Discussion of Results

OBJECTIVE 1- security challenges due to BYOD adoption facing universities in Kenya and measurers put in place to tackle them.

The questionnaire sought response on a number of BYOD issues besides challenges and measurers that were put in place to tackle the challenges. This was because the researcher wanted a broad feel of the actual situation of BYOD in the selected universities. The researcher will however only restrict the discussion of the results to the following aspects:

a) Negative Impacts (challenges) of BYOD to University Campuses

The researcher wanted to find out how BYOD impacted the operation of the Universities negatively. The response from the ICT administrators was as shown in Figure 20.

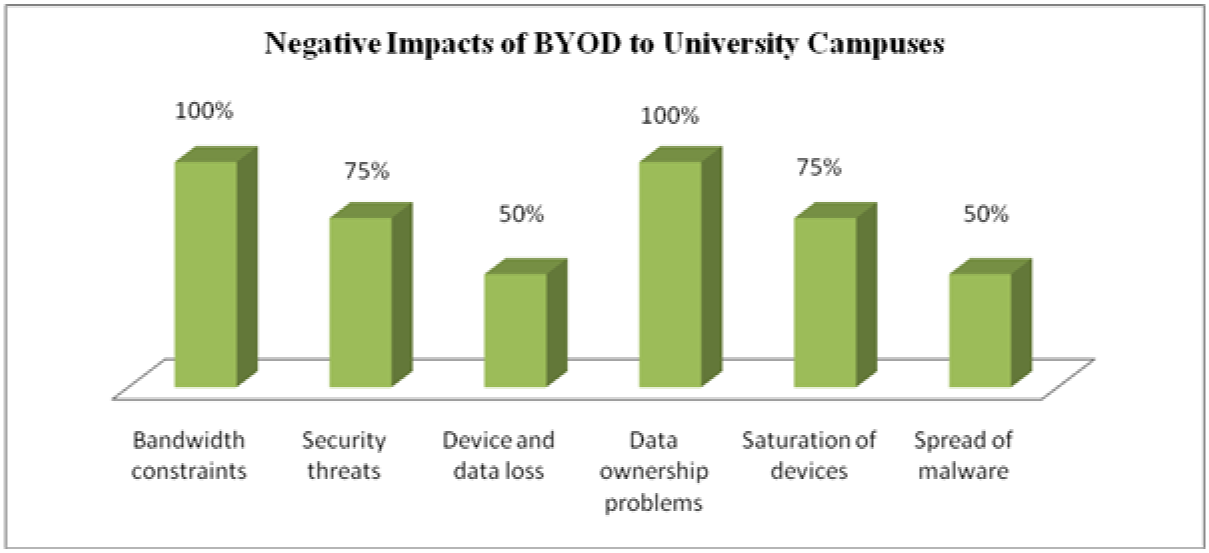


Figure 20: Negative Impacts (challenges) of BYOD to University Campuses

100% of the respondents indicated that BYOD introduced bandwidth constraints, 75% of them indicated that it exposed campuses to security threats, 50% of the respondents indicated that device and data loss was a negative impact, 100% of the respondents indicated that data ownership was problem associated with the adoption of BYOD, 75% of the respondents indicated that the saturation of devices was a negative impact to the operation of the Campus network and 50% of them indicated that BYOD led to spread of malware in the campus network.

Based on the responses given by the ICT administrators it is notable bandwidth constraints is a negative impact in all the universities. This is attributed to the bandwidth acquired by the university (costly) versus the number of users in the universities. The other notable negative impact was the data ownership problems. This is attributable to university data being held in members of staff own devices. Spread of Malware through mobile devices was a negative impact in 5 universities of the 10 sampled and in this regard the researcher felt that spread of Malwares was a serious challenge that ought to be addressed by his proposed framework.

b) Presence of Measures in Place to Address the Negative Impacts(challenges) of BYOD

The researcher sought to know whether the selected universities had put any measurer(s) to try to address the negative impact(s) brought about by BYOD. 75% of the respondents stated that they had **NO** measurer(s) to address the negative impacts while only 25% of the respondents had measurer(s) to address the negative impacts of BYOD that they were experiencing. For the respondents that gave a YES response it was noted that devices access (user log in and authentication), ordinary firewalls and antiviruses were the only measurers adopted to try to address the impact(s). According to the researcher these measures were inadequate to fight against the challenges brought about by BYOD. The proposed framework would therefore be of much help to the universities if adopted.

c) Security Attacks as a Result of Adopting BYOD

The researcher sought to find out the actual attacks on their systems as a result of adopting BYOD. The response from the ICT administrators was as shown in Figure 21.

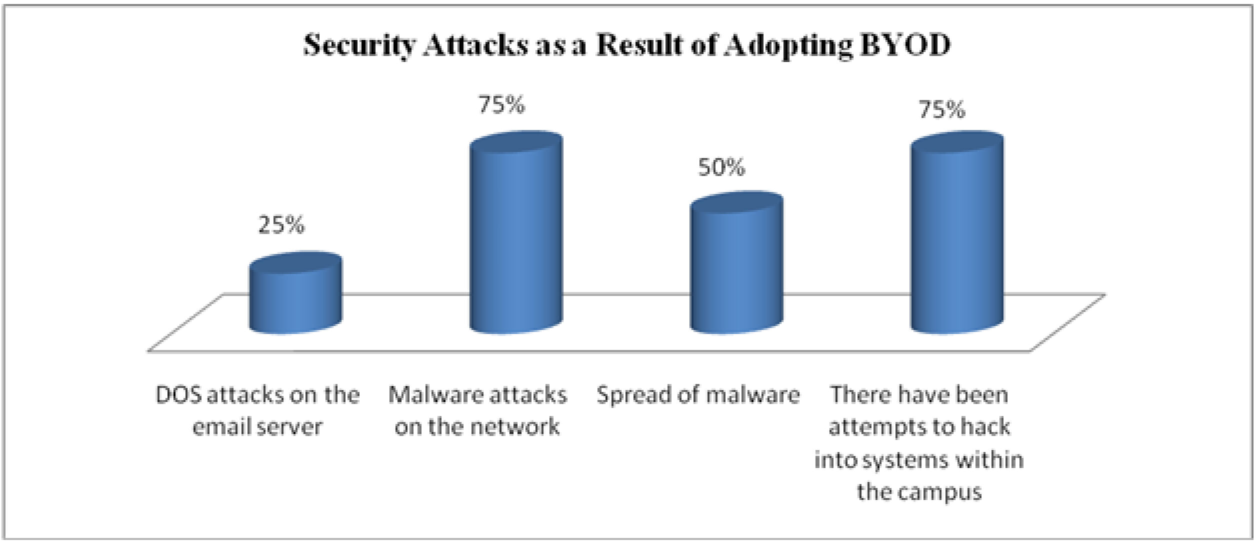


Figure 21: Security Attacks as a Result of Adopting BYOD

From the response it was noted that malware and its spread to other devices and systems was the major attack that the selected universities faced. Attempts to hack into Campus servers were also another notable attack. These attacks were evidently powered and facilitated by insecure mobile devices that were in connection to the campuses network and inadequate security measures to address BYOD threats.

OBJECTIVE 2-Review of existing BYOD Frameworks

The review of existing BYOD framework and other solutions was done in literature review (2.4). The review was based on 5 goals that were proposed by (Ocano, Ramamurthy and Wang, 2015). The results of the review were captured in table 1 in item 2.4.2. Based on the review BSF framework was adopted and was modified to address the following shortcomings that were missing in the framework:

- Device access to the enterprise network-an elaborate and secure access of mobile devices into the campus network.

- Malware invasion-malware installed into mobile devices with an aim of attacking internal systems and other mobile devices.
- Rogue access points, WLAN adhoc functions in smart phones and hotspot applications in laptops- disabling of WLAN adhoc-tethering and hotspots in smart phones and hotspot applications such as connectify in laptops to avoid unauthenticated connection of other mobile devices through the authenticated ones.

OBJECTIVE 3- To develop an advanced devices access BYOD security frameworks that will guide universities to securely adopt BYOD.

KANYI BYOD security framework was developed and its detailed functioning and components integration was captured in items 3.6 and 3.7. The framework was designed and illustrated as shown in Figure 3. Figure 3 shows the general outline of the components of the framework and how they are connected to each other.

The network model to integrate the framework components to the campus network was also designed and illustrated as shown in figure 4. Figure 4 captures the design of the implementation of the framework in the campus network. The theoretical quantification of the security vulnerability associated with the framework was done using CVSS version 2-item 4.2.1.

The results of the quantification were captured in table 10. The framework was “partitioned” into paths through which the attacker would use to invade the campus servers and systems. The graph of the attack paths was shown in figure 5. The graph assisted the researcher to know where vulnerabilities of the framework existed and how the attacker could penetrate to the campus servers and systems.

OBJECTIVE 4-To test and validate the framework

The framework was designed in OPNET modeler and an attacker node (mobile node) introduced. The attacker node launched DOS (ping floods) attack to the campus network. Simulation was done based on the three scenarios highlighted in chapter 5. Various aspects of the performamnce of the network and its components based on the 3 scenarios were measusred and the results were as follows:

a. **Database application(entry) of the campus server**.

The database server response rate from a genuine mobile node 2 was captured. The simulation of the response rate between the server and mobile node 2 for the 3 scenarios was as captured in figure 13. It was noted that database response rates went high when the DOS attacker was introduced. This was expected due to the fact that the network became congested by the ping flood packets from the attacker mobile node. When preventive measurers were introduced (MDM firewall) to tackle the DOS attack the response rates went back to the expected levels.

b. **HTTP(web service) application of the Campus server.**

The web server response rate to the mobile node 2 were measured and the simulation results were captured in figure 15. It was noted that web service response rates went high when the DOS attacker was introduced. This was expected due to the fact that the network became congested by the ping flood packets from the attacker mobile node. When preventive measurers were introduced (MDM firewall) to tackle the DOS attack the response rates go back to the expected levels.

c. DNS server CPU performance.

The CPU performance of the Campus DNS server was analysed and the results of the utilization analyses simulation captured in figure 16. It was noted that DNS CPU utilization in percentage per second went high when the DOS attacker was introduced. This was expected due to the fact that the DNS was engaged by the ping flood packets from the attacker mobile node. When preventive measurers were introduced (MDM firewall) to tackle the DOS attack the DNS CPU utilization rates went down to the expected levels.

d. WLAN media access delay.

The delay in accessing the WLAN media from mobile node 2 was measured and the simulation results captured in figure 17. It was noted that it took longer to access the WLAN media when the attacker node was introduced. This was as a result of the congestion of the network brought about by the ping flood packets from the attacker node. It was further noted that the WLAN media access delay was higher when MDM firewall was introduced as compared to when none was in existence because the firewall added to the delay of the WLAN media access as well.

e. Core Switch B traffic flow to and from Campus server

The flow of network traffic through core switch B to and from Campus server was measured for the three scenarios. The simulation results were as captured in figure 19. It was noted that the switch was much busy-much network traffic when the DOS attacker node was introduced. This was expected due to ping flood packets from the attacker which increased the network traffic to high levels. When preventive measurers were introduced to tackle the DOS attack the network traffic through the core switch reduced to become the least as shown in the figure due to few packets coming from the mobile nodes to the campus server.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

Conclusions from the simulation of the framework as well as findings from the ICT administrators of the sampled universities will be given in this chapter. Recommendations by the researcher to the universities will also be given in the same chapter.

5.2 Conclusions

According to the ICT administrators that were used as respondents BYOD security attacks and challenges were in existence in their campuses. Little measurers to address security attacks and challenges brought about by BYOD adoption had not been put in place. Its was evident BYOD was in use in all universities sampled and hence measurers to address the challenges and attacks they experienced was extremely necessary.

The other frameworks fell short in addressing or were not very clear on how devices would access, prevent anuthorized access of other devices through rogue access points and detection and spread of malwares through mobile devices. The proposed framework elaborated very clearly how security threats and challenges and data ownership problems would be addressed. Universities lacked mechanism to prevent attacks on their servers from the connected mobile devices. The proposed framework was clear on the Campus servers access and attack preventive measurers from members of staff and students.

From the simulation done it was noted that the security threats brought about by mobile devices that were in connection was significant and could not be ignored at any single moment. The simulation showed that servers could easily be compromised by external and internal attackers by use of mobile devices. It is therefore extremely necessary for universities and other non academic institutions to put in place security measurers to prevent themselves from threats and attacks that originate from mobile devices. BYOD threats are dynamic and therefore the security measurers put in place should evolve with the vulnerabilities detected and attacks techniques applied.

The proposed BYOD framework is very effective to address many BYOD threats if it is implemented by academic institutions where mobile devices are in heavy use by students and members of staff. The proposed MDM agent that is installable to mobile devices before they are permitted to connect to the campus network play a foundation security role at the devices level from where security threats and attacks originate from and effective management of campus owned data on mobile devices.

5.3 Recommendations

Mobile devices have expanded the scope of attack to the campus network servers and systems. To have no plan of secure access, usage of mobile devices and transfer of data to and from the mobile devices is a recipe for disaster. BYOD is a worldwide accepted movement and therefore the sooner the institutions embrace security measurers to address BYOD threats and attacks the better for them.

Universities and other learning institutions are the highest consumers of BYOD and therefore the biggest victims of BYOD attacks. The researcher would therefore recommend that learning institutions adopt the proposed BYOD framework to ensure that they rip the full benefit of BYOD and keep themselves safe from BYOD threats and challenges.

5.4 Contribution to Knowledge and Justification of Universities as a Case Study

The researcher chose to universities as a case study because BYOD is more pronounced and is in heavy use in institutions of higher learning and hence BYOD threats and challenges would be more pronounced in them. The BYOD threats and challenges could be similar to other non academic institutions but would be more and most frequent in institutions of higher learning due to the extensive use of personnaly owned mobile devices. Therefore universities and other institutions ought to be in the forefront in the fight against BYOD threats and challenges.

This research has contributed to BYOD framework solutions by introducing advanced devicess access and monitiring and has addressed rogue access points as a loop hole used for unauthorized devicess access to the institutions' network. Categorization of users from mobile devices so that permissions could be assigned to them not to access specific servers has also contributed to the advancement of BYOD frameworks as solutions to the fight against BYOD security threats and challenges.

REFERENCES

1. Scarfo, A., 2012, November. New security perspectives around BYOD. In *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on* (pp. 446-451). IEEE.
2. Calder, A., 2013. Is the BYOD movement worth the risks. *Credit Control J*, *34*(3), pp.65-70.
3. Wood, A., 2012. BYOD: The Pros and Cons for End Users and the Business. *Credit Control*, *33*(7/8), pp.p68-70.
4. Ghosh, A., Gajar, P.K. and Rai, S., 2013. Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), pp.62-70.
5. Miller, K.W., Voas, J. and Hurlburt, G.F., 2012. BYOD: Security and privacy considerations. *It Professional*, *14*(5), pp.53-55.
6. Markelj, B. and Bernik, I., 2012. Mobile devices and corporate data security. *International Journal of Education and Information Technologies*.
7. Morrow, B., 2012. BYOD security challenges: control and protect your most sensitive data. *Network Security*, *2012*(12), pp.5-8.
8. Thomson, G., 2012. BYOD: enabling the chaos. *Network Security*, *2012*(2), pp.5-8.
9. Armando, A., Costa, G., Verderame, L. and Merlo, A., 2014. Securing the" Bring Your Own Device" Paradigm. *Computer*, *47*(6), pp.48-56.
10. Dahlstrom, E. and diFilipo, S., The Consumerization of Technology and the Bringing your Own Everything (BYOT) Era of Higher Education, Education Report (2013).

11. Boon, G.L. and Sulaiman, H., 2015. A review on understanding of byod issues, frameworks and policies. In *3rd National Graduate Conference (NatGrad2015), Universiti Tenaga Nasional, Putrajaya Campus. Retrieved from http://cogs. uniten. edu. my/portal/NatGrad2015/conference. html*.

12. Kamau, W.T., 2013. *The bring your own device phenomena: Balancing productivity and corporate data security* (Doctoral dissertation, University of Nairobi).

13. MBALANYA, M.E., 2013. *Bring your own device and corporate information Technology security: case of firms listed on the Nairobi Securities exchange limited* (Doctoral dissertation, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI).

14. Drury, A. and Absalom, R., 2012. BYOD: an emerging market trend in more ways than one. *Employee attitudes to work/life balance drive BYOD behavior, Logicalis white paper, ovum*.

15. Navetta, D. and Paschke, C., 2012. Bring your own device security and privacy legal risks. *Information Law Group LLP*.

16. Hernandez, A. and Choi, Y., 2014. Securing BYOD Networks: Inherent Vulnerabilities and Emerging Feasible Technologies.

17. Mansfield-Devine, S., 2012. Interview: BYOD and the enterprise network. *Computer fraud & security*, *2012*(4), pp.14-17.

18. Ocano, S.G., Ramamurthy, B. and Wang, Y., 2015, February. Remote mobile screen (RMS): An approach for secure BYOD environments. In *Computing, Networking and Communications (ICNC), 2015 International Conference on*(pp. 52-56). IEEE.

19. Leavitt, N., 2013. Today's Mobile Security Requires a New Approach. *IEEE Computer*, *46*(11), pp.16-19.

20. Wang, Y., Wei, J. and Vangury, K., 2014, January. Bring your own device security issues and challenges. In *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th* (pp. 80-85). IEEE.

21. Russello, G., Conti, M., Crispo, B. and Fernandes, E., 2012, June. MOSES: supporting operation modes on smartphones. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (pp. 3-12). ACM.

22. Andrus, J., Dall, C., Hof, A.V.T., Laadan, O. and Nieh, J., 2011, October. Cells: a virtual mobile smartphone architecture. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles* (pp. 173-187). ACM.

23. Titze, D., Stephanow, P. and Schütte, J., 2013, March. A configurable and extensible security service architecture for smartphones. In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* (pp. 1056-1062). IEEE.

24. Chung, S., Chung, S., Escrig, T., Bai, Y. and Endicott-Popovsky, B., 2012, December. 2TAC: Distributed access control architecture for" Bring Your Own Device" security. In *BioMedical Computing (BioMedCom), 2012 ASE/IEEE International Conference on* (pp. 123-126). IEEE.

25. "Cisco BYOD Smart Solution," Cisco, 2013. [Online]. Available:http://www.cisco.com/web/solutions/trends/byod smart solution/docs/byod smart solution aag.pdf

26. Zhao, Z. and Osono, F.C.C., 2012, October. "TrustDroid™": Preventing the use of SmartPhones for information leaking in corporate networks through the used of static

analysis taint tracking. In *Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on* (pp. 135-143). IEEE.

27. **https://nvd.nist.gov/vuln-metrics/cvss**

APPENDIX 1

QUESTIONNAIRE USED TO ACHIEVE OBJECTIVE 1

This questionnaire is to collect data on BYOD security threats and measurers taken to address them in universities in Kenya. This is to address one of my objectives in my research project.

Kindly note that this questionnaire will only be used for the academic purpose of undertaking this project.

IS BYOD in practice in your campus by both staff and students?

□ Yes

□ No

Indicate which of the following positive and negative impacts have been brought about by BYOD to your campus

Positive Impacts of BYOD to your Campus

□ Productivity improvement by staff

□ Transfer of cost of purchase and maintenance of devices to the staff

□ Few computer labs due to students owning personal devices

State any other positive impact(s) brought about by BYOD to your campus if there are any

Negative Impacts of BYOD to your Campus

□ Bandwidth constraints

□ Security threats

□ Device and Data loss

□ Data ownership problems

State any other Negative impact(s) brought about by BYOD to your campus if there are any.

Do you have measurers in place to address the negative impact of BYOD highlighted above?

□ Yes

□ No

If yes state what has been done to address the negative impacts brought about by adoption of BYOD in your campus

Do you have a means of tracking how many personally owned devices are in connection to the Campus network and the activities they are doing on the campus network?

□ Yes

□ No

What security attack(s) have your campus received as a result of adopting BYOD?

What was done to address the attack(s)?

What technology procedures have your campus put in place to safeguard itself from BYOD security threats?

State the technology being used in your campus to enhance or support BYOD.

Does your campus have a general Information Technology security policy in place?

□ Yes

□ No

Does your campus have a BYOD security policy in place?

□ Yes

□ No

In relation to BYOD have the following issues been addressed technologically in your campus? If yes state how.

- BYOD in relation to Cloud Computing
- Data and Device ownership
- Secure access Controls
- Mobile services permitted on personally owned devices
- Trust of mobile devices
- Mobile devices compliance with BYOD security policy.

Thank you for your kindness to respond to this questionnaire.