Identity and Authentication Model for Bring Your Own Device in Organizations

The University of Nairobi
School of Computing and Informatics

OBOTE ADRIAN VICTOR
P53/6524/2017

Supervisor: Dr. Andrew M. Kahonge

A research project submitted in partial fulfilment of the requirements of the degree of Master of Science in Distributed Computing Technologies

MAY 2019

DECLARATION

This research project is my original work and has not been submitted for a degree in any other university.

Signature: _____ Date: _____

OBOTE ADRIAN VICTOR

This project has been submitted to the University for Examination with my approval as the University Supervisor

Signature _____ Date: _____

Dr. Andrew M. Kahonge

School of Computing and Informatics

University of Nairobi

ABSTRACT

The use of personal mobile devices for work related assignments and vice versa has become a common trend in business today. With escalated developments in technology, there has been a significant shift on how organizations and employees carry out business which has necessitated the adoption of new practices such as Bring Your Own Devices (BYOD). The research sought to review existing BYOD implementation models in device identity management and user authentication in organization and outline the challenges that face organizations in implementing BYOD strategies. It was found out that many organizations have implemented different models that address BYOD challenges from the perspective of the device, data and/or application. However, it was noted that illegitimate access to organizations' systems via the use of legitimate devices and applications by unauthorized users remained a challenge that exposed organizations to unprecedented uncertainties. It was also established that the adoption of BYOD in organizations was low due to a number of reasons that were noted to centre on information security and privacy concerns. This research work developed and tested a prototype that combined device identification and user authentication in an augmented model as a proof of concept and a means of experimentation to address the security and privacy challenges that various implementations have had in the implementation and adoption of BYOD in organizations.

ACKNOWLEDGMENT

I give all the glory to God.

TABLE OF CONTENTS

List of Tables

List of Figures

Abbreviations

BYOD – Bring Your Own Device

ISACA - Information Systems Audit and Control Association

IP - Internet Protocol

MAC - Media Access Control

OTP – One Time Password

PERMIS - Privilege and Role Management Infrastructure Standards

SQL –Structured Query Language

TLS - Transport Layer Security

UAR – User Access Repository

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Technological advancement has significantly changed the way business is conducted in the computing industry. The introduction of BYOD to work environment has revolutionized the provision of services to end users with an emphasis on the independence of time and location. While technology has eased doing business, it has also introduced risks that threaten the business from various facets.

In its publication, audit giant Ernst and Young (2013) highlighted that portable devices with scalable computing power make them convenient to use on real time basis. However, the devices are vulnerable to physical lose and network security breaches, hence posing a danger to the data they contain. It thus follows that while there is the advantage of an employee accessing business information on the go, there is also the risk of the data security and privacy loss in the unfortunate event that the devices get accessed by unauthorized individuals. Consequently, organizations that incorporate the BYOD should bring into focus the risks as well as the rewards involved (Voas, Miller, and Hurlburt, 2012).

Many organizations that have already adopted the BYOD technology have had to change their information security architecture to accommodate these improvements. The key changes that continue to determine the viability of BYOD include:

i. Definition of a network security perimeter

   Traditional network security defined network security in terms of physical location of the technology equipment and the ownership of assets. Technology has since collapsed the walls of physical location and the definition of the perimeter moved just beyond physical access to who and what can access an enterprise's wealth of data. Therefore, the new security perimeter definition centres on users, their devices and the data of the enterprise. Organizations have to adopt to these changes in the technology space for them to remain competitive in business.

ii. Definition of information security policy

   Increasing demand for flexible working hours and the adoption of BYOD is having a massive impact on how organizations react to information security. BYOD may provide greater flexibility and increased productivity due to the round the clock accessibility of corporate data. It has also caused a shift in information technology consumerization, where personal devices are interfacing with corporate data. Organizations must, therefore, consider how their

infrastructure cope with the increased number of devices accessing the network, ensuring that employees' devices are adequately secured and not breaching the company's policies, hence the redefinition of information security policies.

Organizations must focus on the leverage that BYOD yields to the business as well as security threats the same technology poses. The models that are adopted by different organizations must ensure that the definition of network security parameters and policies focus on users, their devices and data. Existing BYOD implementations are not able to uniquely identify a user device and its legitimate user before granting access to resources. Many organizations have implemented different models that address BYOD challenges from the perspective of the device, data and/or application. Illegitimate access to organizations' systems through legitimate devices and applications by unauthorized users remains a challenge that exposes organizations to unprecedented uncertainties.

1.2 Problem Statement

As most businesses incorporate the concept of BYOD, security and privacy are the major risks faced by both the organization and their employees. Businesses are particularly concerned with corporate data security and how user behaviour would affect their data. On the other hand, the employees would concentrate on the privacy and confidentiality of their personal data on devices they use for business related activities as well as the rights employers have over their personal data.

With the security and privacy concerns around the concept of BYOD, tremendous effort has been made to ensure that businesses operate in a secure and safe environment bearing in mind the vulnerabilities and numerous threat vectors that organizations are predisposed to. Many organizations have implemented different models that address these BYOD challenges from the perspective of the device, data and/or application. However, illegitimate access to organizations' systems via the use of legitimate devices and applications by unauthorized users has remained a challenge that exposes organizations to unprecedented uncertainties. This is a security gap that needs to be closed since the exposure through identity theft may result in security breaches.

Therefore, it is incumbent that as technology brings into focus the concept of BYOD to organizations, the identity of a user to access data via a network is authoritatively confirmed while at the same time protecting the privacy and confidentiality of the user's private data.

1.3 Research Objectives

(i) To review existing BYOD models to fill research gaps in mobile identity management and user authentication.

(ii) To identify factors that influence device identity management and user authentication for BYOD in organizations.

(iii) To develop an integrated device identity and user authentication model for organizations.

(iv) To test the proposed BYOD model for device identity and user authentication management.

1.4 Justification

The adoption and implementation of the concept of BYOD in organizations is fast changing the way businesses operate. While it is enriching business prospects, it is also posing a myriad of security and privacy challenges prompting continuous research in this area. BYOD implementations have borne increased threats to information assets, hence the need to identify risks, threats and suitable mechanisms to prevent and mitigate the impact of security attacks on information assets.

It has been noted that the research approach in this area mainly focused on the adoption and implementation of the concept of BYOD. However, this research shifted to address the security and privacy challenges that various implementations have had in device identity and user authentication, and then propose a solution that would seek to combine device identification and user authentication in an augmented model which would guarantee in-depth security in the BYOD environment.

1.5 Scope of Research

As businesses become more reliant on technology and BYOD infiltrates corporate institutions, the floodgates of data leakage and threats open up. BYOD is an attractive business model with numerous considerations. This research specifically concentrated on device identification and user authentication, which limited the frames on which literature review was conducted and the manner in which the research design was articulated. The emphasis was to research on ways in which an organization's ICT department can provide a full identity spectrum to management when the concept of BYOD is implemented in a business.

Further, this research focused on the ability of BYOD to work and its implications on information security as a global concern. The research identified global trends used to prevent, mitigate and reduce the impact of information security threats where the use of employee owned devices in enterprise settings is concerned.

CHAPTER TWO: LITERATURE REVIEW

Protecting data from unauthorized access is a technical challenge that IT security faces as a growing number of employees use their own devices to access their employers' systems. A detailed review of current adoptions and implementation strategies of the concept of BYOD will establish the context of the research study. Specific literature review emphasis was based on understanding the concept of BYOD, empirical review of significant past studies done on its benefits, as well as the security risks and threats that the concept of BYOD brings to organizations.

2.1 Concept of BYOD Adoption in Organizations

The concept of BYOD traces back to the increased and continued development of the integration of technology with businesses. Giant technology firms have been able to continuously modify electronic devices to meet customers' demands so as to remain competitive. Introduction of advanced features that are able to handle office duties on electronic hand-held devices has made it possible for employees to become more interested and active in handling office tasks using their personal devices. Moreover, the concept of BYOD has enabled employees to transition between business and personal tasks seamlessly, hence encouraging employees to work when they are most motivated.

It was noted that individuals often have multiple devices that rarely match any preconceived ideas and standards in an organization. Therefore, as IT departments in organizations drive technology, the contemporary revolution has changed the culture such that users are the ones getting the latest, cutting edge technologies first, and they want to bring those technological advancements using their devices to work (Brandly, 2011).

A survey conducted by ISACA (2011) notes that fifty-four percent of employees have a personal device they use for work. Employees enjoy the freedom the BYOD scheme offers, and company balance sheets look healthier for the minimized hardware it spends on. Brandly (2012) notes that various organizations have not only grown to tolerate the use of personally-owned and user-liable devices at the work place, but also encouraged and sponsored it. However, the convenience of BYOD has also raised significant data security risks.

2.2 BYOD Information Security Considerations

Willis (2012) states that the best strategy that Information Technology can use to deal with the opportunities that are presented with the rise of BYOD as well as the risks that come along with it is to address it comprehensively. This would entail policy formulation, software installation, infrastructure controls, and proper information security education and application management.

A report by Fortinet (2012) outlines that most organizations address BYOD challenges through custom and explicit policies that are highly relevant to their implementation needs. It enumerates examples where some organizations limit their access to data or applications while others require their employees to have specific device brands and software installed on their devices to admit those devices into the corporate network.

The concept of BYOD is largely viewed from a wide spectrum of information security due to its complexity and hidden implications that advance beyond the ownership of the device. There are various factors that are considered by organizations as they adopt the BYOD concept in their daily operations.

2.2.1 User Privacy

While organizations adopt the concept of BYOD, of importance to the organization is the safety of information that may be contained in the devices that the employees use or the overall infrastructure where the organization stores its data. Businesses put emphasis on the activities of the employee on the mobile device and the data which is accessed with the view of monitoring such activities. Privacy policy, therefore, informs what should be monitored, the actions that a privileged system user can have on the whole architecture of BYOD and under what circumstances.

2.2.2 Device Choice

This entails user preferences of various devices available in the market. An organization will consider the majority of devices their users can afford, or have already purchased while instituting the security baseline.

2.2.3 Liability

Organizations want to hold their employees legally responsible for the actions that happen to the organization’s data in their devices. This captures the elements of baseline protection for enterprise data on BYOD devices, access liability for personal usage of the device both online and offline during and outside working hours.

2.2.4 Technical Specifications

An organization should consider the capacity and architecture of existing infrastructure and wireless networks to accommodate an influx of devices once the concept of BYOD is adopted. Further, the organization should consider the resources that user devices have access in its network.

2.3 Existing BYOD Adoption Models and Architectures

2.3.1 Integrated Model for BYOD Adoption

Different needs of an organization determine the model that the organization would consider in adopting a model for the implementation of BYOD (Alberta Education, 2012). Figure 1 below shows this model in which the organization uses standardization and flexibility metrics to categorize the adoption of personal devices.

On one extreme of the spectrum, employees must acquire a specific single type of device that has been standardized while on the other end, employees are at liberty to use devices of their choice.

1	2	3	4
Limit personally owned devices to specific brand/model	Limit personally owned devices to specific technical specifications	Limit personally owned devices to specific capabilities re: software, tools, apps, etc.	No limitation on personally owned devices, provided they are Internet-ready

Figure 1: Integrated model for BYOD Adoption by Alberta Education

An integrated model provides four different flavours that an organization may choose from while implementing BYOD as enumerated below:

(i) Limit personally owned devices to specific brands/models – While the organization would have knowledge of the capabilities of the devices they are dealing with, restriction to device preferences makes it difficult to implement this model.

(ii) Limit personally owned devices to meet specific technical specifications – The user may have any device, but the device must conform to a restricted requirement for it to be allowed to access resources in the organization's network. In this flavour, technical support to the various device platforms poses a challenge in case of technical incapacity.

(iii) Limit personally owned devices to specific capabilities – This flavour is more flexible, but less standardized in that user devices are restricted to perform specific functionalities. This

option is relatively inelastic to users who may not be necessarily technology savvy to identify devices that meet the requirement of the functionality that the organization may require.

(iv) No limitation on personally owned devices, provided they are internet-ready – Users are allowed to use any device as long as it can connect to the internet. However, Alberta (2006) points out that the downfall is that users may become incapable of utilizing their devices due to pedagogical requirements, hence affecting their ability to work with their devices.

2.3.2 Hybrid model of BYOD Adoption

This model (figure 2) borrows heavily from the four flavours of the integrated model. The hybrid framework is basically a combination of any two categories from the integrated model, making it vary depending on the combination selected. The key advantage of this model is that it significantly takes into consideration the infrastructure of the underlying organization (Mwenemeru, 2013).

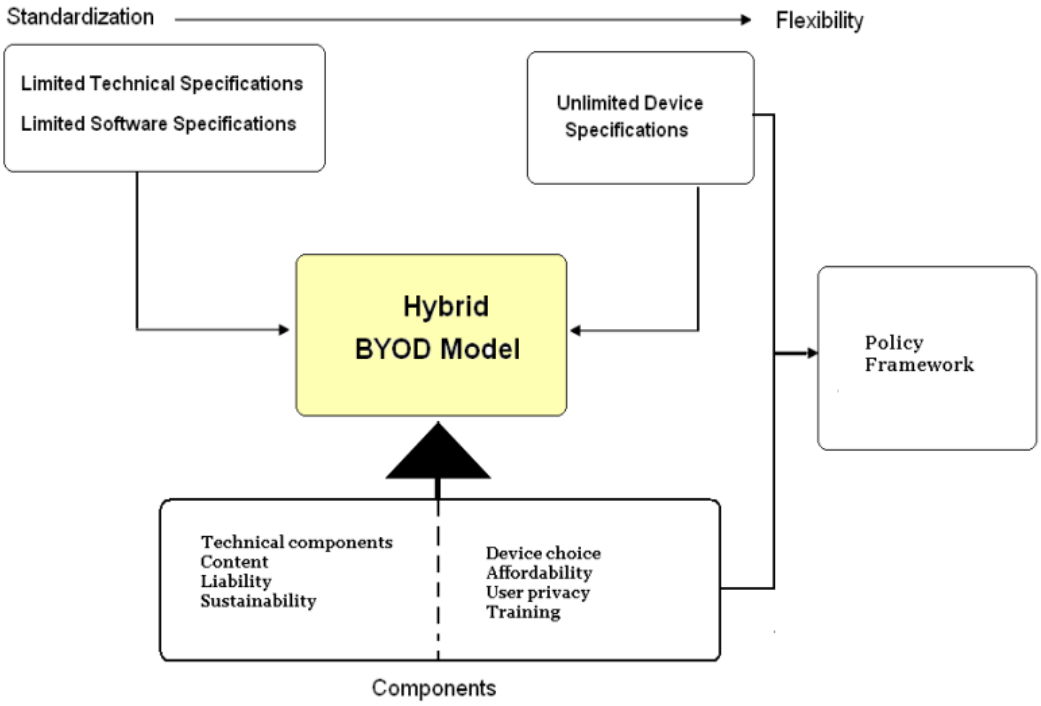

Figure 2: Hybrid model for BYOD Adoption

In addition to the standardization and flexibility aspects of the integrated model, this model was also guided by different components of BYOD security considerations. It served as a solution to some of the key challenges that were likely to sprout from standardization and flexibility as well as device components requirements. However, this model posed a challenge as the organization was likely to lose control of its information and data. Further the model did not outline comprehensive

evaluation criteria which specified which devices were allowed and how employees were notified that their devices satisfied that criteria.

2.3.3 Akenti: Certificate-based Authorization

Public Key Infrastructure emphasizes on providing secure means of authenticating identities using cryptography. It is, however, silent on processes that need to be followed when authorizing identities to perform an action in an environment. Thompson, Abdelilah, and Srilekha (2003) propose a model as shown on figure 3 to establish identity of devices in a distributed environment based on an X.509 standard called Akenti, which defines the formats of public key certificates.

Akenti authorizes devices to access distributed resources based on pre-identified users and access policies that have been generated on certificates signed by X.509 identified stakeholders.

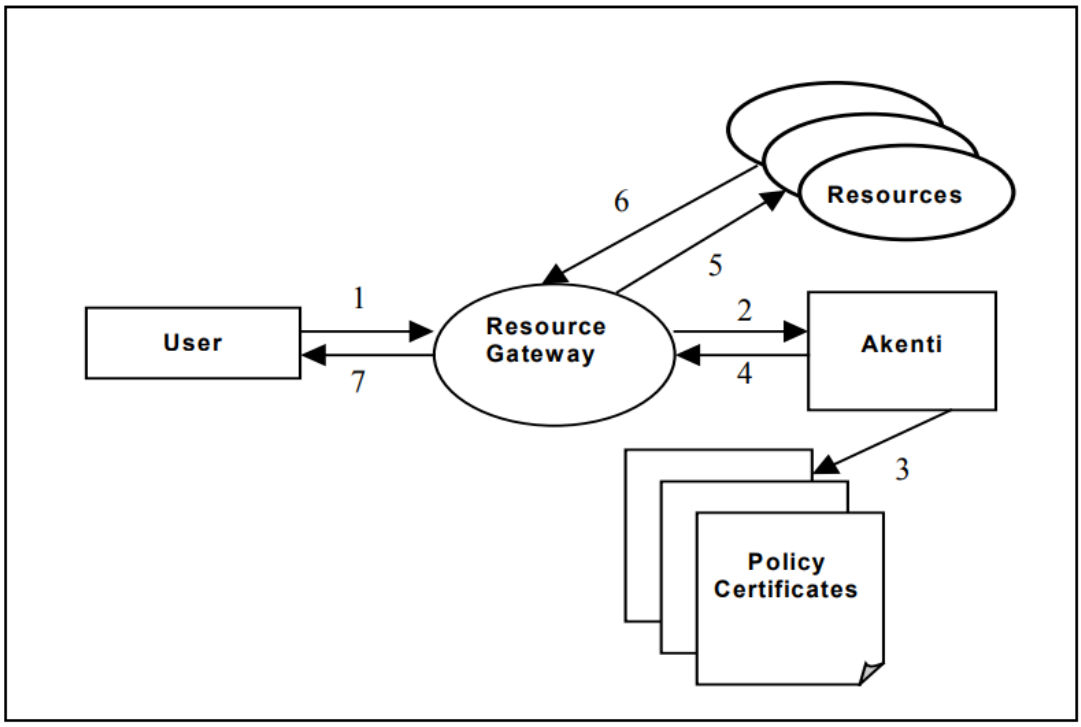

Figure 3: Akenti - Certificate-based Authorization Model

The development of the Akenti model was based on the X.509 standard to identify devices, and relied on Transport Layer Security (TLS) to establish secure connections between users and organizations in a distributed environment. In this model, access constraints are stored as signed certificates on the Akenti policy engine, making it simple and transmission of data easy. However, since all these policy statement are stored in one place, integration of new ones is difficult especially in large organizations with many devices. Further, device identities are directly linked to

the permissions that are allowed to the device on the policy statement, making it vulnerable to inconsistencies and fragmentation.

2.3.4 PERMIS: Role-Based Access Control

Otenko Chadwick and Ball (2003) propose a role-based access control for remote devices using X.509 standard where role assignment is distributed widely across an organization. In this model, locally based policy certificates are used to determine which roles are trusted and which privileges are granted to a user.

This model has two subsystems as demonstrated on figure 4 – Privilege Allocation and Privilege Verification. The former issues role assignment to attribute certificates that it signs to users, in addition to issuing them with application specific authentication tokens. The latter authenticates and authorizes the remote user before granting access to the target. PERMIS is an attribute-certificate-based authentication model which is complex in nature since the resource provider must send defined policies to the repository.

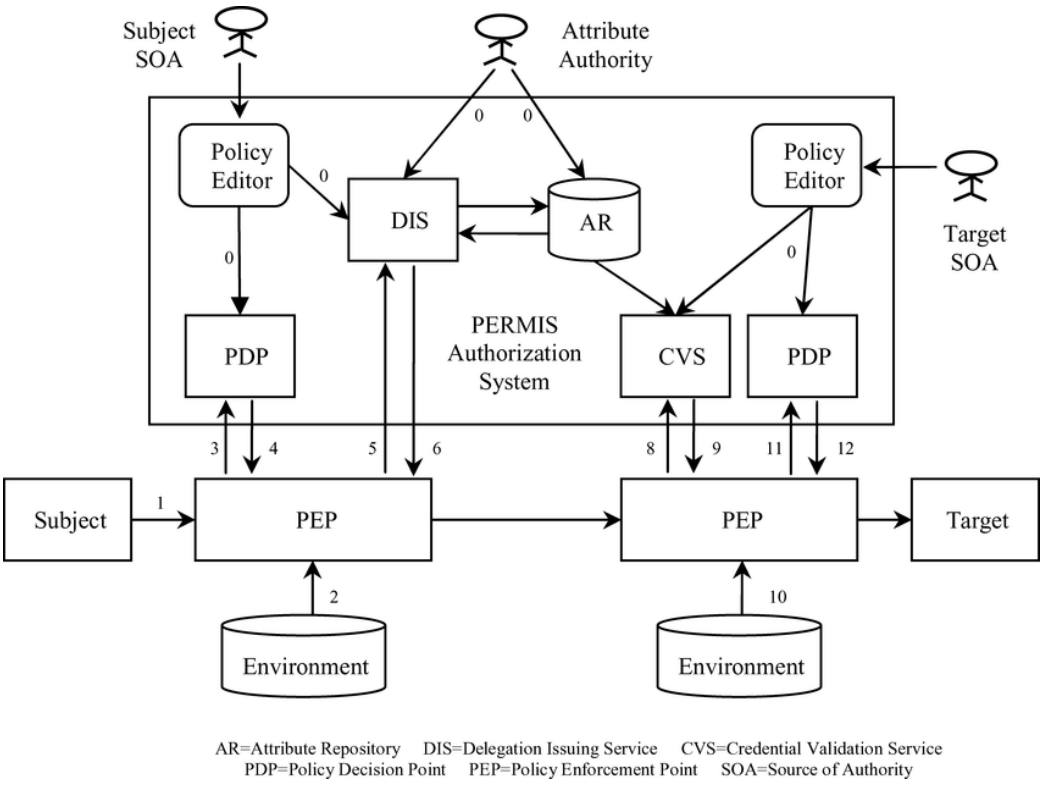

Figure 4: Components and authorization model of PERMIS

2.4 Conceptual Model

The conceptual model outlined on figure 5 below consists of the device user and the system administrator. The model has a pre-registration of user devices made by the system administrator who captures the username, password and unique identifier assigned to device (MAC address). The model is conceptualized such that when a user requests access to an organization's resources, the user is prompted to enter a username and password that are then compared with those that were pre-stored in the User Authentication Repository (UAR). The verification engine then confirms whether the combination of username and password match the MAC address pre-registered in the UAR and belong to the user requesting access. Once the verification occurs, the authenticator prompts the Code Generator to send a one-time code to the pre-registered user's mobile number that is keyed in the device interface before access to the resources is authorized via the access control register which determines what the authenticated user can do to the organization's resources.

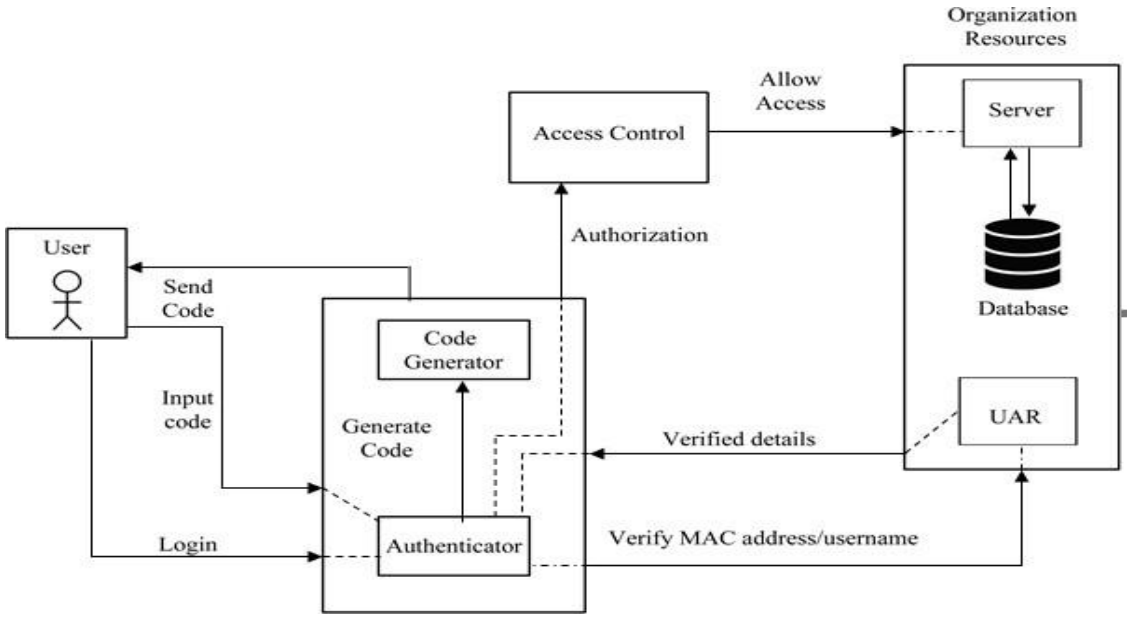

Figure 5: Conceptual Model

CHAPTER THREE: RESEARCH METHODOLOGY

Research methodology incorporated how data was gathered and analyzed, in order to meet the criteria set out in research questions as well as attain the intended objectives that were to address device identity and user authentication management. This section, therefore, delved into the research methodology used and how it was applied in solving the research problem.

3.1 Research Design

Research design is described as the logic or master plan on how the research was to be conducted. It outlined how all of the major parts of the research work together in an attempt to address the research questions. Parahoo (1997) describes a research design as "a plan that describes how, when and where data are to be collected and analyzed". Research design is similar to an architectural outline in that it is an actualization of logic in a set of procedures that optimizes the validity of data for a given research problem. This research therefore viewed research design as the general plan of what the researcher did to answer the research questions. An appropriate and well-executed research design ensured that this was done in the most rigorous way possible.

This study used a descriptive research design to obtain information regarding the current status of BYOD implementations in organizations. The use of descriptive research fitted into this research because description uncovered existing gaps on the concept of BYOD in organizations. The research enumerated facts as they currently exist.

Descriptive research design was important because it provided important facts and understanding about the identity and authentication of personal devices in organizations. It ensured the researcher had a closer look into happenings, behaviour, practices, methods and procedures. It also provided information which served as a basis for scientific judgement. The common means of obtaining data while applying descriptive research design include the use of questionnaires, personal interviews with the aid of a study guide or interview schedule, and observation, either participatory or not. This research focused on the use of questionnaires that were distributed across different organizations in different industry sectors.

While the research focused on descriptive research design, it also used explanatory research design methods. This was important because it also explained why organizations are facing challenges with BYOD implementations using existing models.

3.2 Data Collection and Analysis

The concept of BYOD is rapidly spreading across many organizations in Kenya and the world at large. Personal computing devices are now very affordable and competition has necessitated many firms to adopt BYOD to increase employee productivity, work flexibility as well as reduce expenditure on devices. Therefore, this research targeted organizations within Nairobi, Kenya because of its proximity to the researcher, limitation of time and the fact that the city has many organizations that have embraced technology and taken advantage of innovations.

The data used in this research was obtained from selected organizations in Nairobi. The use of semi-structured questionnaire and structured questionnaire played a fundamental role in obtaining the required data that was used in the research. Information security managers/officers and System administrators of the organizations were interviewed on the various threats that BYOD has brought to the organization and how the organization was dealing with these challenges. The collected data highlighted the kind of challenges that Information security managers/officers and system administrators experience in the management of BYOD.

According to Peersman (2014), data analysis techniques must be selected to match the specific assessment in terms of its key evaluation questions and the resources available. It goes further to state that the techniques must complement each other's strengths and weaknesses to fill existing gaps with existing data. Therefore, since resources and other factors influence the choice of methods to analyze data, the researcher concentrated on what utilized less resources as well as meeting the intended objectives of the research. Data was analyzed after the first interviews on the information security managers/officers and System administrators, since it made work easier for the researcher.

This research used Microsoft Office Suite to analyze the collected data. This ensured the researcher gained insights on the concept of BYOD, thus enabling the researcher to conceptualize the best way of addressing the challenges that organizations face in implementing BYOD.

3.3 System Design and Architecture

System design entails defining the different elements of a solution such as the architecture, modules and components, as well as the different interfaces of those components together with the data that goes through that system. It is meant to satisfy a business or organization's specific needs and requirements through engineering a coherent and well-running system. System design details the proposed model design and architecture by incorporating user requirements collected through

interactions with potential users and industry experts. Design diagrams were used to bring out design elements. The requirements were obtained from potential end users using semi-structured interviews which were both formal and informal. Secondly, observation of normal staff routines in organizations also played a key role in obtaining data to be used to design the solution.

3.3.1 Functional and Non-functional Requirements

Functional requirements are the intended behaviour of the system that were captured as services, tasks or functions. The proposed solution should:

a) Capture details of the device such as the name, username of the user, phone number of user, IP and MAC addresses.
b) Store details of the device on a centralized database.
c) Verify the username, match it to a MAC address and phone number pre-stored in a database
d) Generate a random one-time code every time a user requests log in
e) Send a random one-time code to the phone number pre-registered when instructed to do so.
f) Verify the validity of the random one-time code when entered
g) Grant access to the authorized resources once authentication has been achieved.
h) Allow the system administrator to access the backend and reset the system or carry out manual authentication of a failed log in.

Non-Functional Requirements were the quality attributes that were considered when developing the proposed solution which were used to evaluate the operations of the solution. Below are some of the attributes that were considered during the development of the proposed solution:

a) Performance – efficient in processing authentication requests such that there are minimal delays.
b) Response time – the entire duration for authentication and validation to allow or disallow access to resources should be within acceptable limits.
c) Usability – the users of the solution should find it easy and simple to learn and comprehend the solution without any technical background.
d) Robustness – any unexpected errors should be handled by the system and proper error messages displayed to assist the user troubleshoot.
e) Reliability – development of the solution should consider the strategy for error detection and correction such that there are minimal failures of the solution while performing its operations.

3.3.2 System Analysis Diagrams

A context flow diagram demonstrates the relationship that the system has with other external entities as a single high-level process. Figure 6 below show the flow of data in and out of the proposed solution.

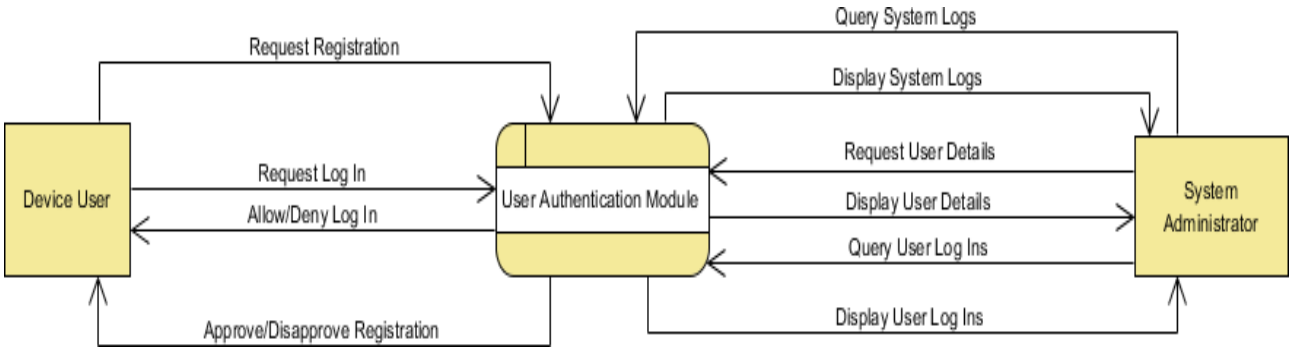

Figure 6: Context flow diagram

It is noted that the main users of the system are the device owners and system administrators. Figure 7 below outlines how these two system operators interact with the system and how data flows from one module to the other. The device owners, upon request to access organizational resources, provide login details for identification. The system then processes the inputs given for verification and then allows or denies access to the user. On the other hand, the system administrator is tasked with managing users who access the system and also perform operational duties such as review system logs for audit purposes.

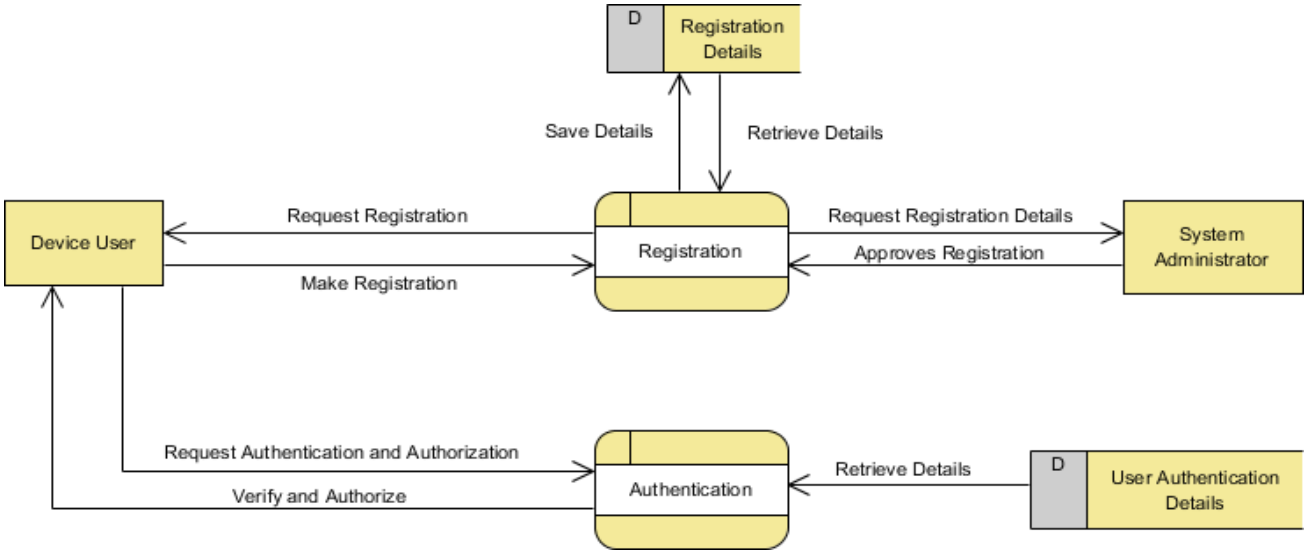

Figure 7: The level 0 Data Flow Diagram

A sequence diagram outlines how a user interacts with the system to gain access to organizational resources. In the successful scenario outlined in figure 8 below, the device user begins by

connecting to the network by entering the username on the log in screen. The authenticator then combines the username and the MAC address associated with the usernames and verifies if this is a valid request. Once confirmed, the code generator generates a one-time random code and sends it to the mobile number registered on the system. This code is time bound and is saved on the authentication repository for the second leg of authentication. Upon receipt of the code, the user enters the code on the device user interface to complete the authentication. The authenticator validates the code and allows access to organization's resources.

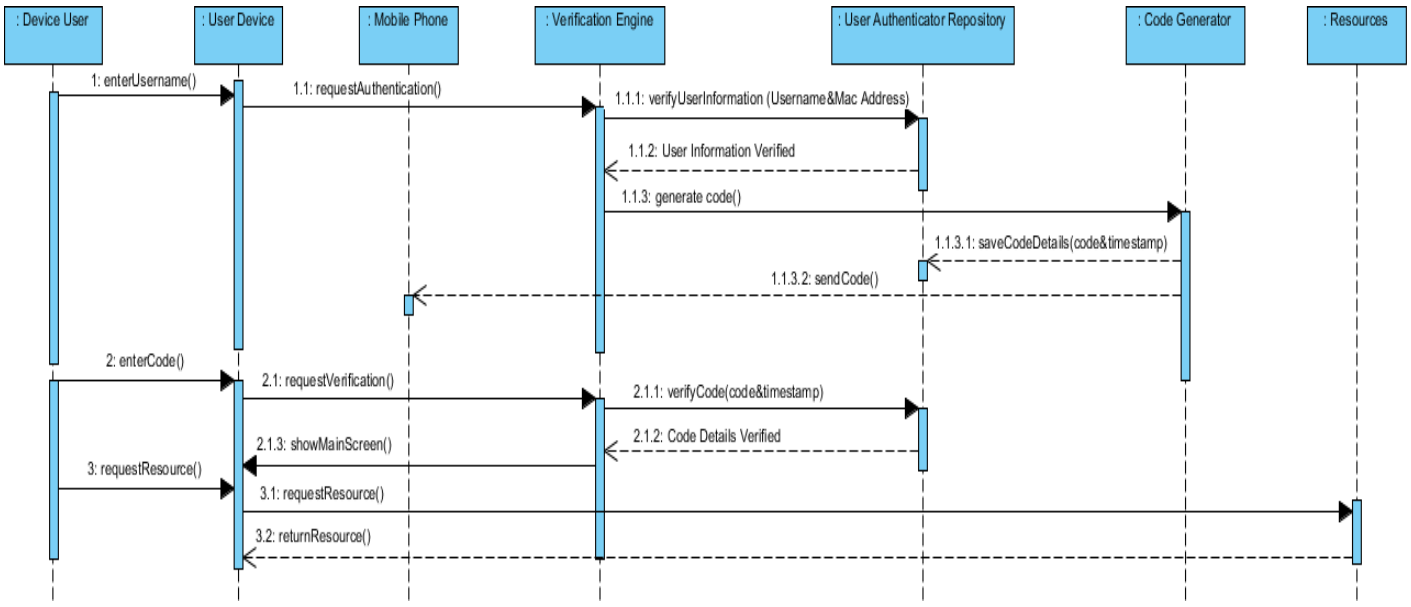

Figure 8: Sequence diagram for device and user authentication

System architecture conceptualizes a solution into a diagram to be able to understand, clarify, and communicate ideas about the structure and requirements that the solution supports. As shown in figure 9 below, the process begins when an end user's device requests access to organizational resources. The user is, thus, prompted to input a username and password on a screen which are then matched to the MAC address on the user's device. These details must have been pre-registered. The username, password and MAC address of the user requesting access are then verified against the pre-registered details on the User Authentication Repository using the Authenticator. The UAR returns the phone number associated with the verified credentials to the Authenticator which then prompts the Code Generator to send a notification in form of a random one-time code which is time-bound to the user to enter on the user interface to be granted access to the requested resources. When this code is entered within the allowed timeframe, the Authenticator validates the device and grants access.

In instances where a user is denied access, upon proper identification, the proposed solution allowed the systems administrator to intervene and resolve any technical challenges that might occur during the process. It was noted that the pre-registration of the devices, username and password is done at the back-end by the system administrator.

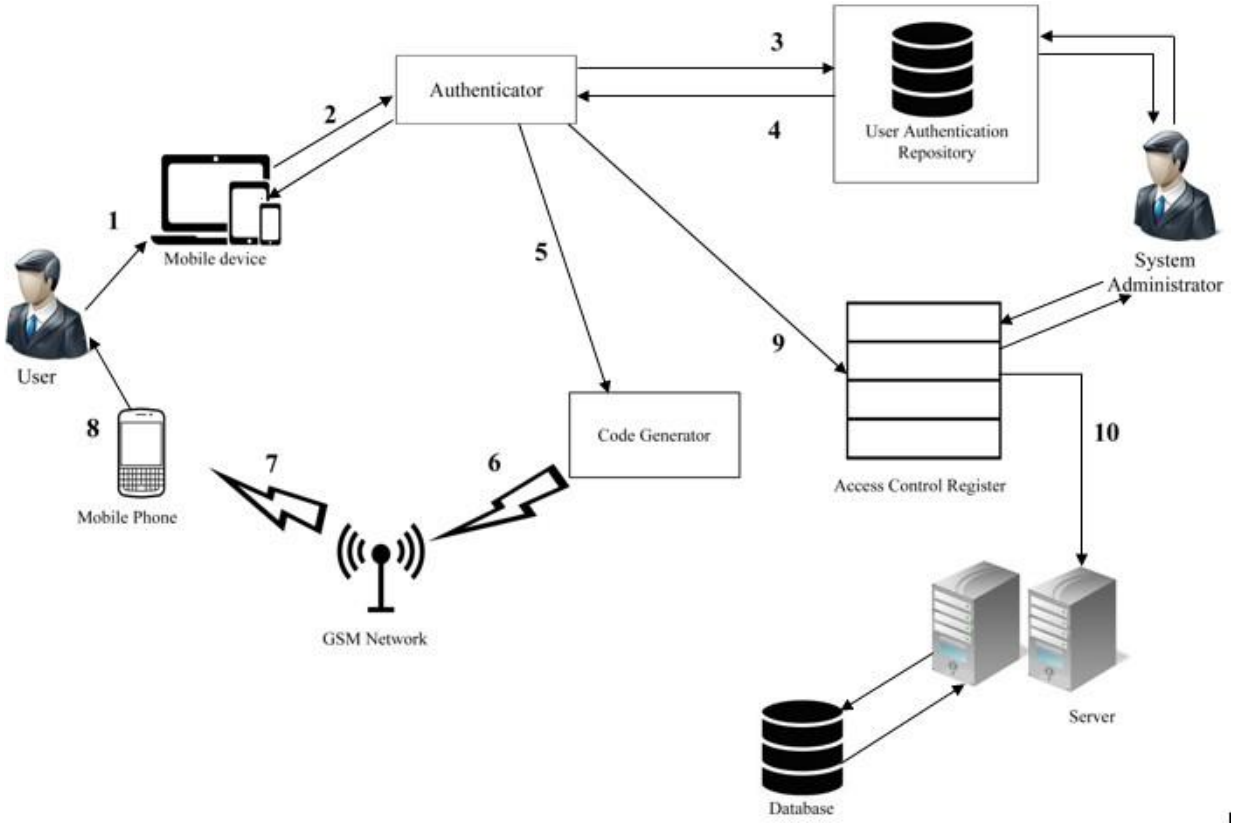

Figure 9: System architecture

3.4 Prototype Development

The prototype was developed using python programming language which is an object oriented language sitting on a Structured Query Language (SQL) database. Python was preferred because it boasts robust power with very clear syntax making it easy to develop the prototype owing to the limited time that the researcher had.

3.4.1 Front End Implementation

The application was implemented such that the prototype was accessed through a web browser where users had to identify themselves on the network by keying in their username and password. Figure 10 below shows the login page for a user to input their registered username and password.

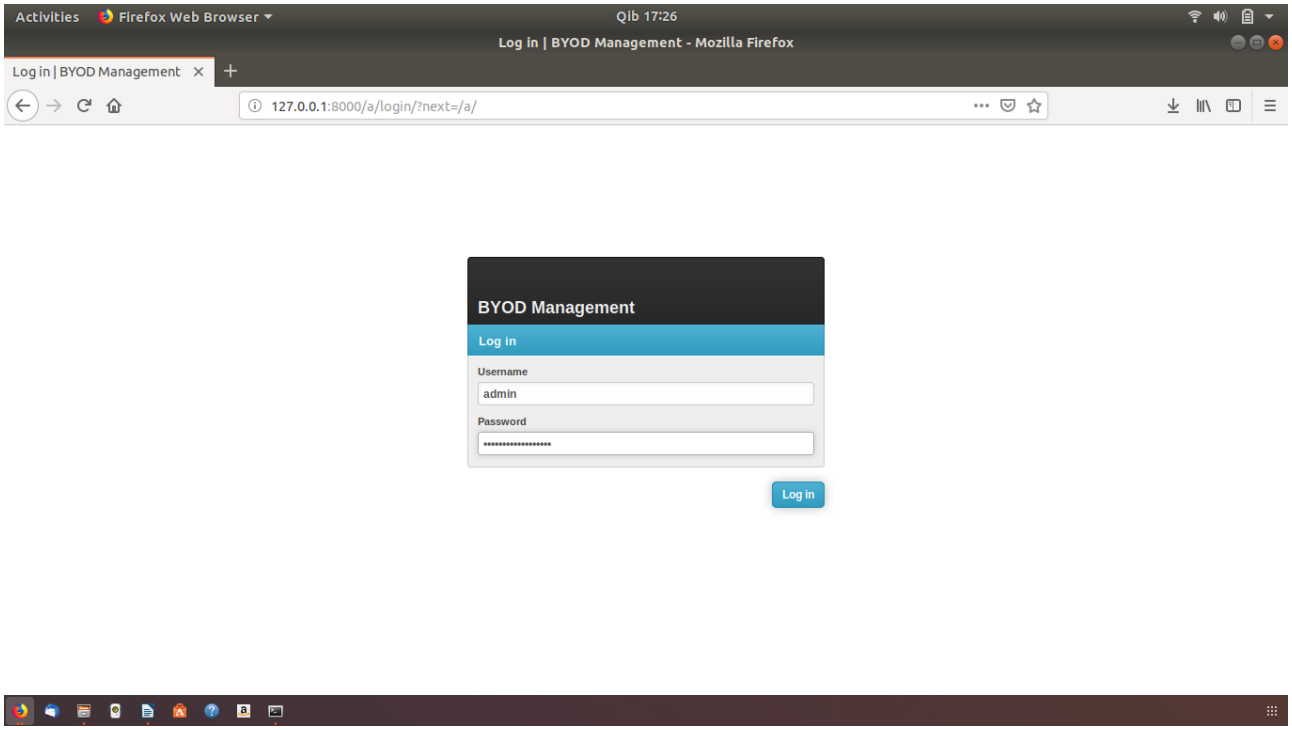

Figure 10: Screen showing identification login

Once the correct pre-registered parameters on the username and password are supplied, the system sends a one-time code to the user's phone number and then displays a screen as shown on figure 11 below which authenticates whether the known user is using a device that had been preregistered.

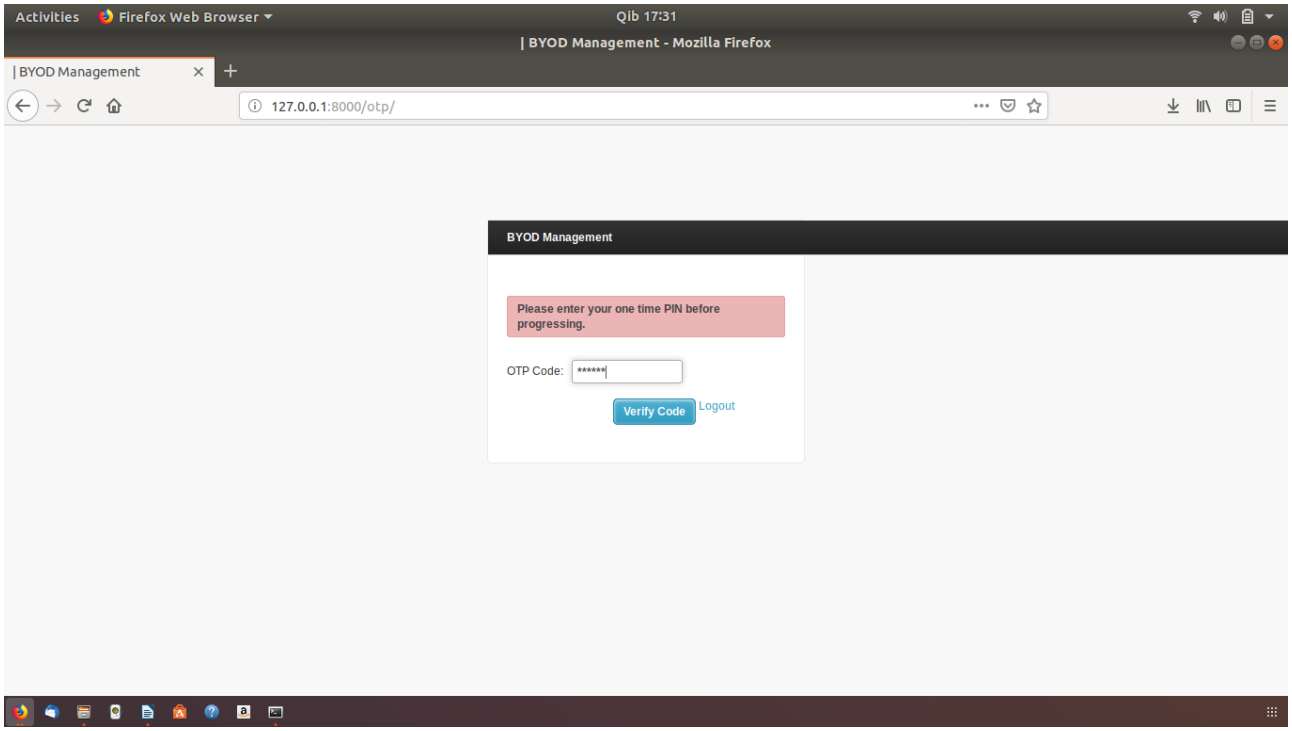

Figure 11: Screen showing authentication login

With the correct one-time code, the system then checks against pre-registered details for the user to be granted access. Figure 12 below shows a successful login by a user who has been granted access after proper identification and authentication.

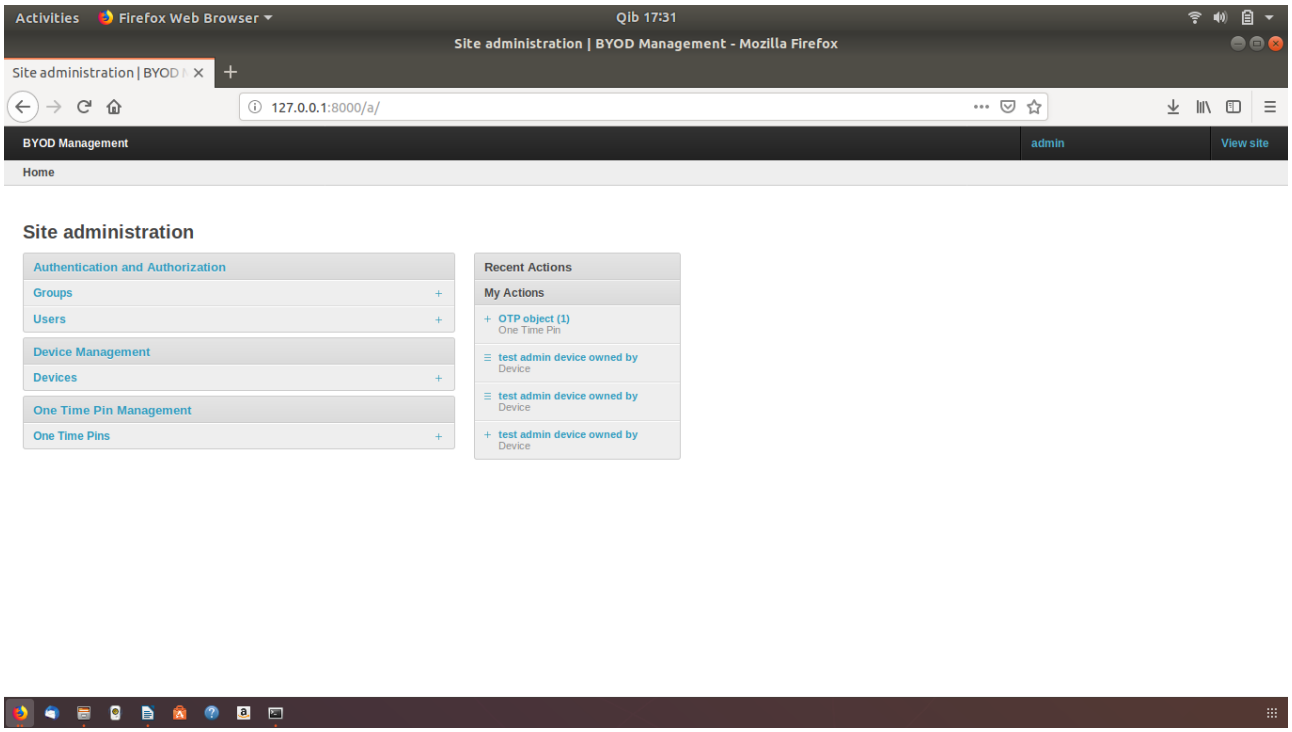

Figure 12: Screen showing prototype dashboard

3.4.2 Back End Implementation

All the back end implementations were designed for the system administrator. The system administrators are responsible for creating user accounts, setting up their security aspects as well as which employees have access to the system. Figure 13 below shows the listing of users who have already been created on the system by the system administrator while figure 14 shows the form that the system administrator uses to manage users on the platform.

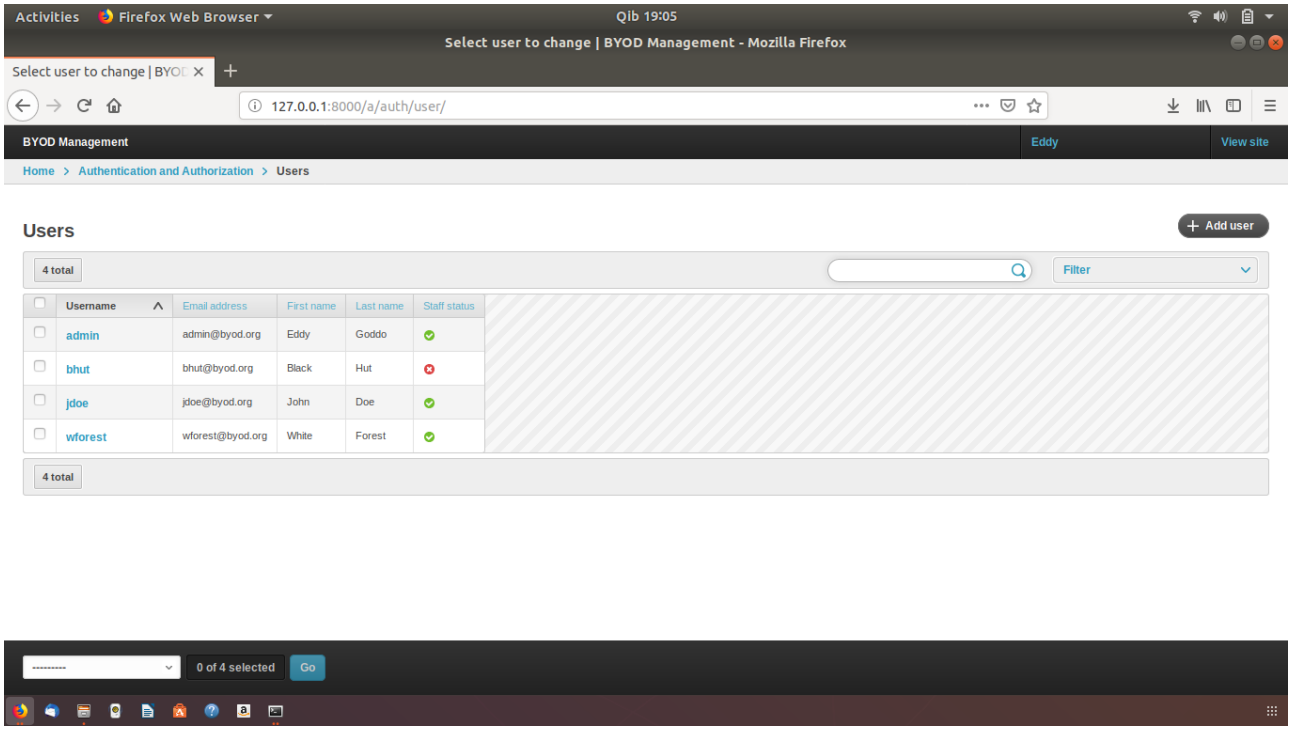

Figure 13: User listing on the system

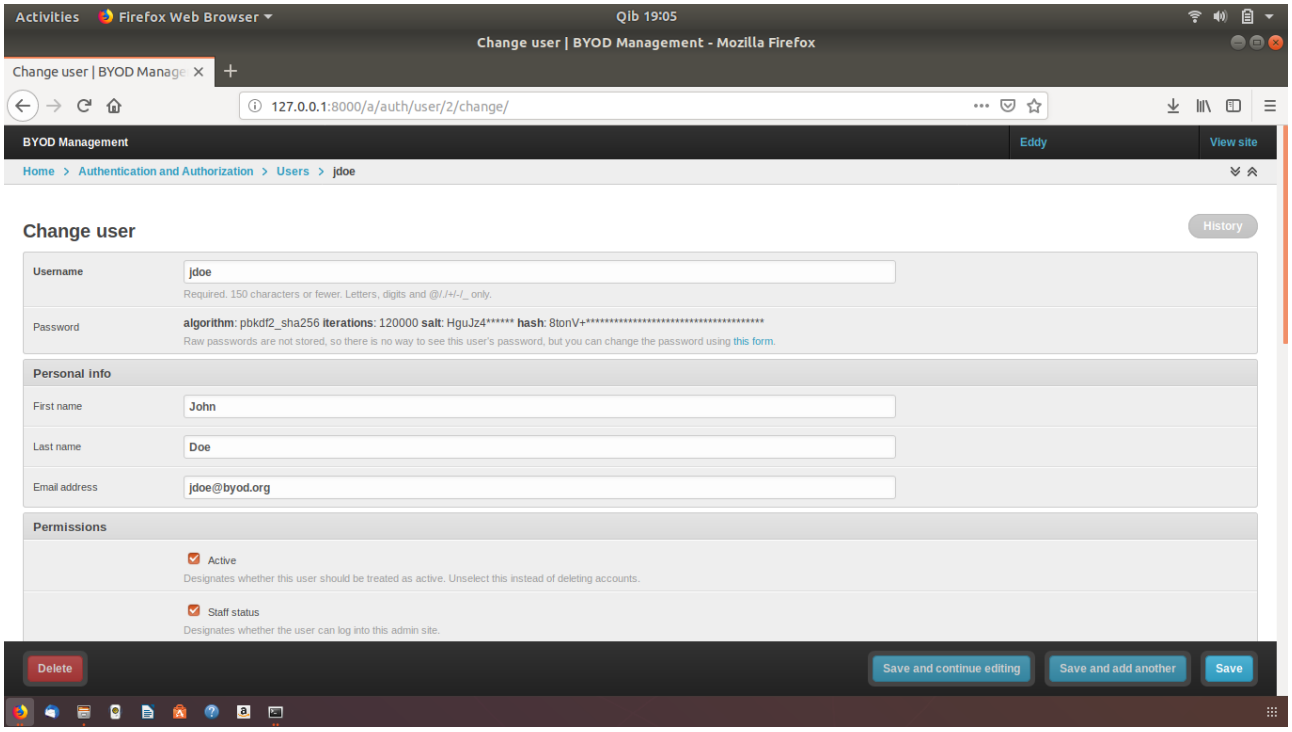

Figure 14: Screen showing user management by administrator

System administrators are also charged with the responsibility of managing devices that access the organization's network and resources. Figure 15 below shows the listing of devices that have

already been allowed to access organization resources by the system administrator while figure 16 shows the form that the system administrator uses to manage devices on the platform.

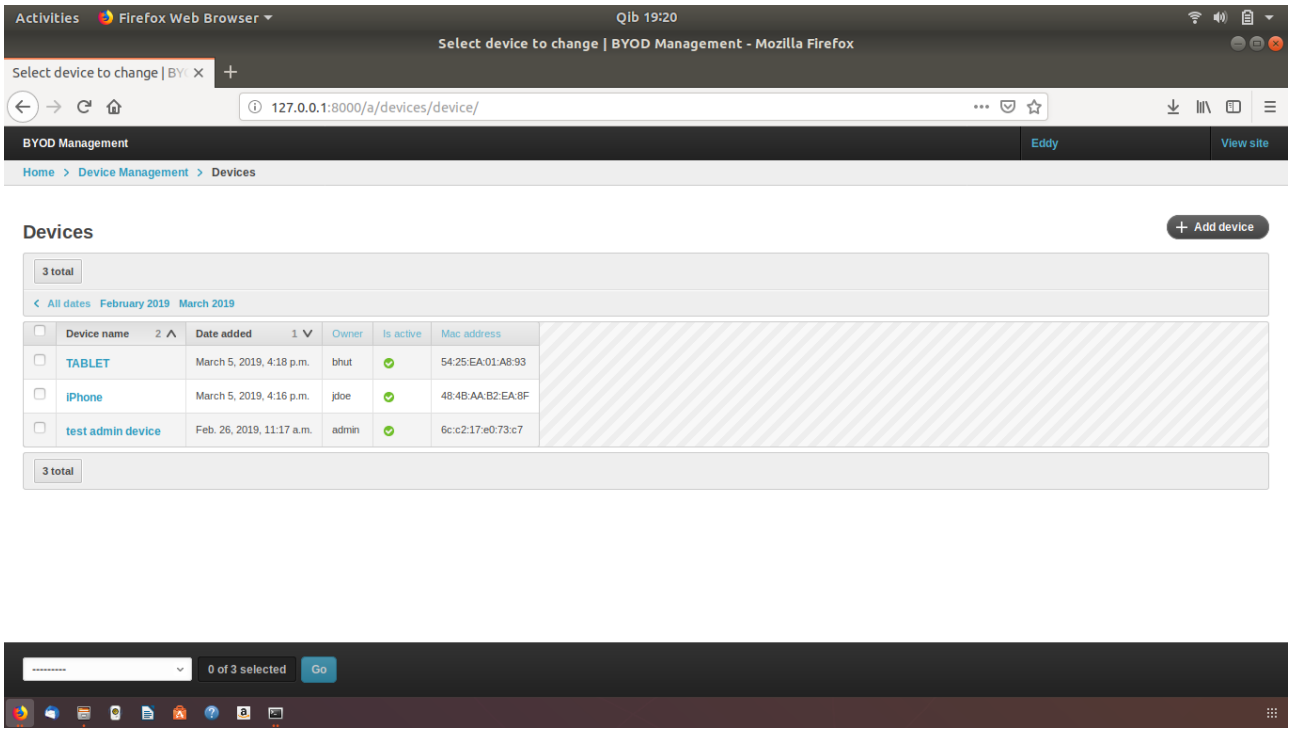

Figure 15: Screen list of pre-registered devices

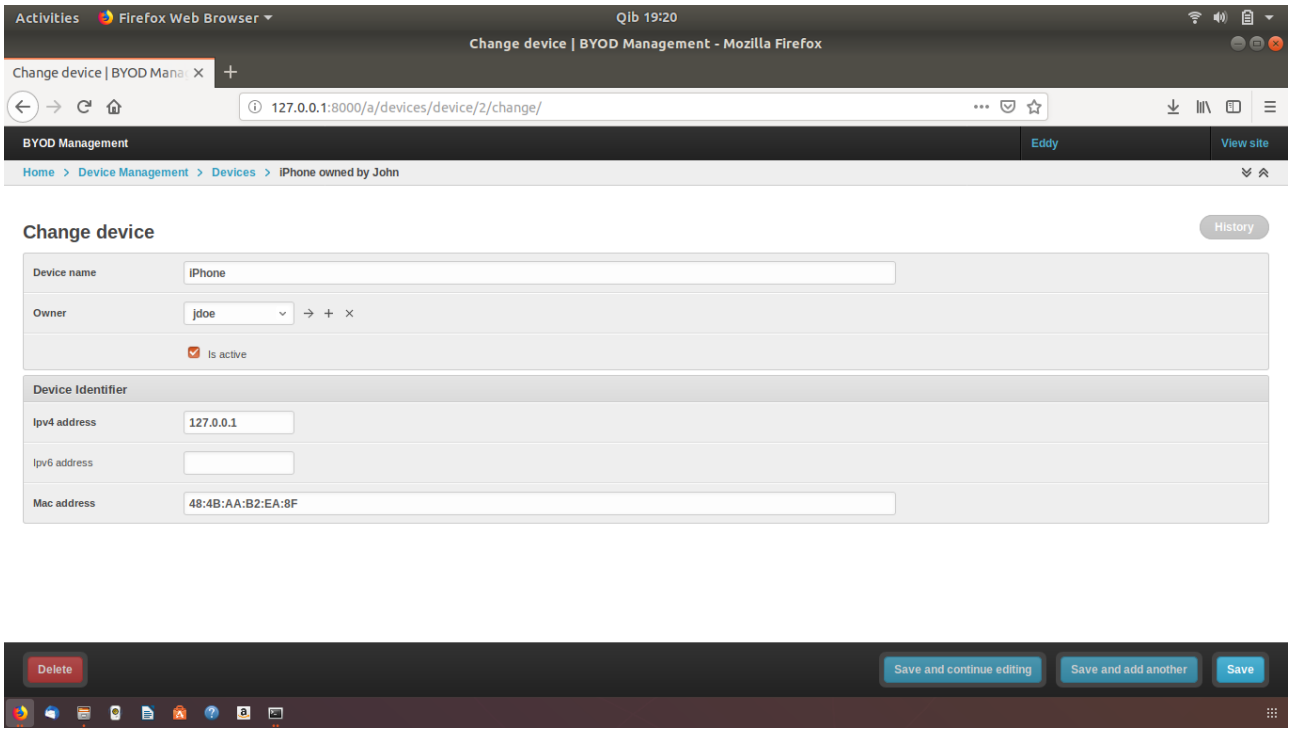

Figure 16: Screen showing device management by administrator

System administrators also register the phone numbers of the users who have been given access to ensure that the one-time code is sent to the correct recipients. On some instances, the employees might change or lose their phone numbers which then will make them not be able to access organizational resources secured on the network. It is for this reason that the prototype as shown on figure 17 below allows the system administrators to have the privilege of changing the user's phone number.

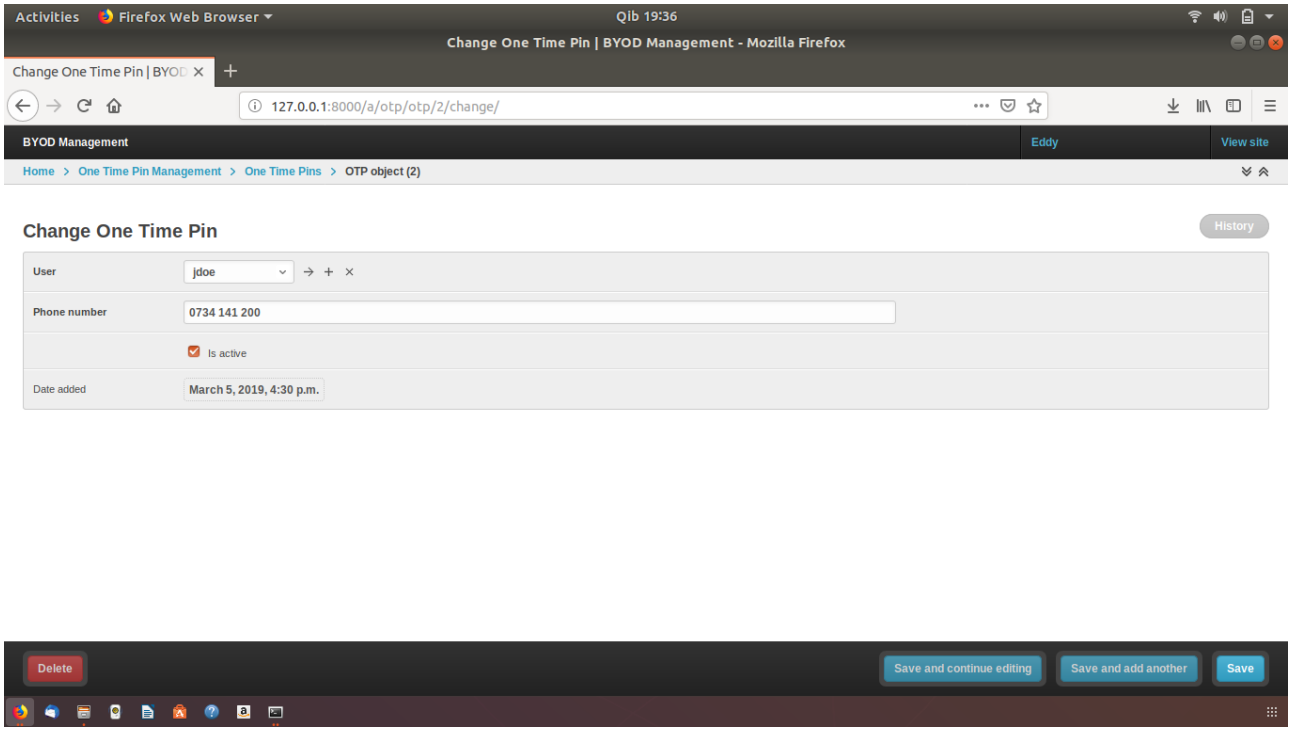

Figure 17: Screen showing OTP management by administrator

3.5 Prototype Testing

Functionalities of the proposed model were tested to verify whether the set research objectives had been met. Test scenarios were formulated and carried out to evaluate the viability of the prototype. All modules that constituted the prototype were tested independently before an integrated test was done on the prototype.

3.5.1 Functional Testing

The researcher adopted an iterative testing methodology where each module was tested as it was being developed. The prototype has two distinctive modules. The first is the administration module where system administrators use the system to manage users, devices and the one-time random code for the users who access the system. The other is the end user module where the users are given a platform to identify and authenticate the devices they are using when they bring their own devices to the workplace.

The two modules of the prototype were subjected to independent testing to isolate each part of the program that may have a bug before fully integrating them. This was the preferred testing technique in this research since it checks individual subprograms, subroutines, classes and procedures in the entire code of the program to demonstrate if there was an error and have it fixed quickly. Test cases were designed and used as outlined on table 1 below.

ID	Page	Test Case	Expected Results	Result
1	Login	User login into portal with Registered username and password	System should display OTP code screen for user to input the random code sent to their phone number	Pass
2	Login	User login into portal with Non Registered username or password	User login should fail with a notification message that the credentials supplied are wrong	Pass
3	Login	User input the correct OTP code sent on the registered phone number	User should be successfully authenticated and be allowed to access the system	Pass
4	Login	User input incorrect OTP code	User should fail to be authenticated with a notification message that the OTP code is wrong	Pass
7	Registration	Administrator allows a user to access the portal	User should be successfully authenticated and be allowed to access the system	Pass
8	Registration	Administrator denies a user access to the portal	User should fail to be authenticated with a notification message that the user is not allowed to access the system	Pass
5	Registration	Administrator allows a device to access organization resources	User device should access the organization resources	Pass
6	Registration	Administrator denies a device access to organization resources	User device should fail to login into the portal with a notification message that the device is not registered	Pass
9	Authentication	Administrator changes MAC address of a device registered to access organization resources	User device should fail to login into the portal with a notification message that the device is not registered	Pass
10	Authentication	Administrator changes phone number of a user registered to access organization resources	• User should not receive OTP code on the previous phone number registered. • User should receive OTP code on the new phone number registered	Pass

11	Authentication	Administrator deletes MAC address of a device registered to access organization resources	System should not allow the Administrator to save the changes made since the MAC address field is mandatory	Pass

Table 1: Summary of sample functional test cases conducted

3.5.2 Non-functional Testing

With the security and privacy concerns around the concept of BYOD, it was noted that tremendous effort has been put to ensure that businesses operate in a secure and safe environment bearing in mind the vulnerabilities and numerous threat vectors that organizations are predisposed to. Non-functional testing was conducted by varying various aspects of the prototype so as to evaluate how it operates with usability metrics as a measure of its readiness for use by different stakeholders.

The prototype was thus exposed to various potential users and their feedback collated and analysed as shown on table 2 below for purposes of this project. The criteria used to pick the metric that was evaluated was based on the non-functional requirements enumerated on the questionnaire used.

ID		Test Case	Expected Results	Result
1	Performance	Efficient in processing authentication requests such that there are no delays	Application load time should not be more than 5 seconds even when multiple users access it simultaneously	Pass
2	Response time	Duration for authentication and validation to allow or disallow access to resources should be within acceptable limits	Application should allow or disallow access within 5 seconds	Pass
3	Usability	Users without a technical background should be able to use the application to access organizational resources	Users should find it easy and simple to learn and comprehend the solution without any technical background	Pass
4	Robustness	Invalid inputs on the systems should disallow access to the system and communicate the reasons to the user	The system should handle unexpected errors and display relevant error messages to assist the user troubleshoot	Pass
5	Reliability	Application should not crash easily when it encounters input errors	Application should have minimal failures while performing its operations	Pass

Table 2: Summary of sample non-functional test cases conducted

CHAPTER FOUR: DISCUSSION OF FINDINGS

Research findings were meant to clarify what the researcher found in relation to both the research questions and existing knowledge. The findings in this research highlighted how the research reflects, differs from and extends current knowledge on the concept of Bring Your Own Device (BYOD) in organizations.

Since the introduction of BYOD is considered a new concept, the research was done based on the respondents' background knowledge. The main characteristics put into consideration during the research were the respondent's age bracket, rank in the organization such as junior or senior staff, the kind and model of devices owned by the respondents, as well as the interactions the respondents had with their personal devices as they conducted their official responsibilities within the organizations. Further, the industry and department that the respondents worked for were also considered.

4.1 Summary findings of Existing BYOD Adoption Models and Architectures

One of the objectives of the research was to review existing models with the aim of enhancing the adoption of BYOD in organizations by developing an integrated model. The researcher reviewed four different implementation models which presented some limitations.

Alberta Education (2012) proposed a model where standardization and flexibility were the metrics that the organization would use to categorize the adoption of personal devices. It was noted that on one extreme, fully standardized devices limited users since not everyone could have the same device. On the other end, fully flexible devices would expose the organization to unknown risks since any personal device could access privileged resources.

Another model that the research reviewed incorporated the standardization and flexibility aspects of personal devices to come up with a hybrid model that could be adopted by different organizations. However, this model posed a challenge as the organization was likely to lose control of its information and data. Further the model did not outline comprehensive evaluation criteria to specify which devices were allowed and how employees were notified that their devices satisfied that criteria.

Akenti was another model that the research reviewed. In this model, it was noted that devices were allowed to access distributed resources based on pre-identified users and access policies that had been generated on certificates signed by X.509 identified stakeholders. Storage of the signed

certificates was done on a single location making it difficult to add new certificates, hence creating a stumbling block to adding new devices to the model.

Finally, the research reviewed PERMIS which is an attribute-certificate-based authentication model. It is a role-based access control tool for remote devices where role assignment is distributed widely in an organization. In the model, locally based policy certificates are used to determine which roles are trusted and which privileges are granted to a user. It was noted that certificate based authentication is complex since the resource provider must send defined policies to the repository, hence making it difficult to implement under ordinary circumstances.

4.2 Summary findings on Extent of Adoption of BYOD Concept in organizations

The research put into consideration the age and type of device the respondents use in their organizations. The respondents were asked to indicate their age bracket so that the researcher can be able to plot the usage of mobile devices in organizations. As displayed on figure 18, it was noted that the majority of staff who participated on research were between 31 and 40 years old, accounting to 44% of respondents. This was followed closely by those who were between 21 and 30 years, comprising of 32%. Therefore, this shows that most organizations that have adopted BYOD are in the youthful age bracket.

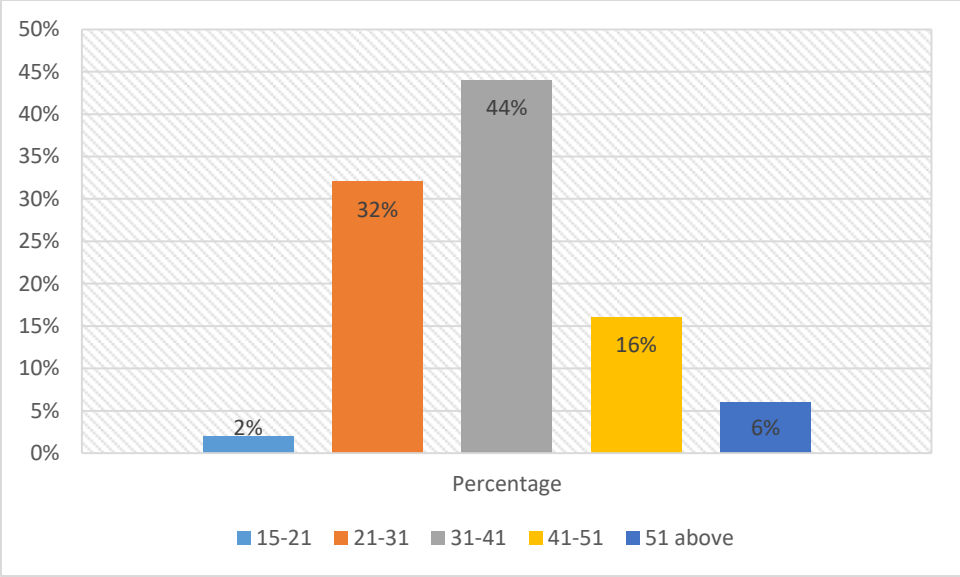

Figure 18: Age distribution of usage of BYOD in organizations

The respondents were asked to indicate whether they use personally owned devices such as smartphones, tablets and laptops in carrying out organizational responsibilities. The objective of this question was to find out if the organizations allow individuals to access privileged resources of the organization using personal devices. Figure 19 shows distribution staff who were allowed to use

personal devices for official business. The majority of the respondents, about 73%, confirmed to have been allowed to use personal devices to transact official responsibilities. However, 23% were not allowed by their organizations to use personal devices for official responsibility. A marginal 4% of the respondents did not answer this question on the questionnaire and the research did not explore further explanations.

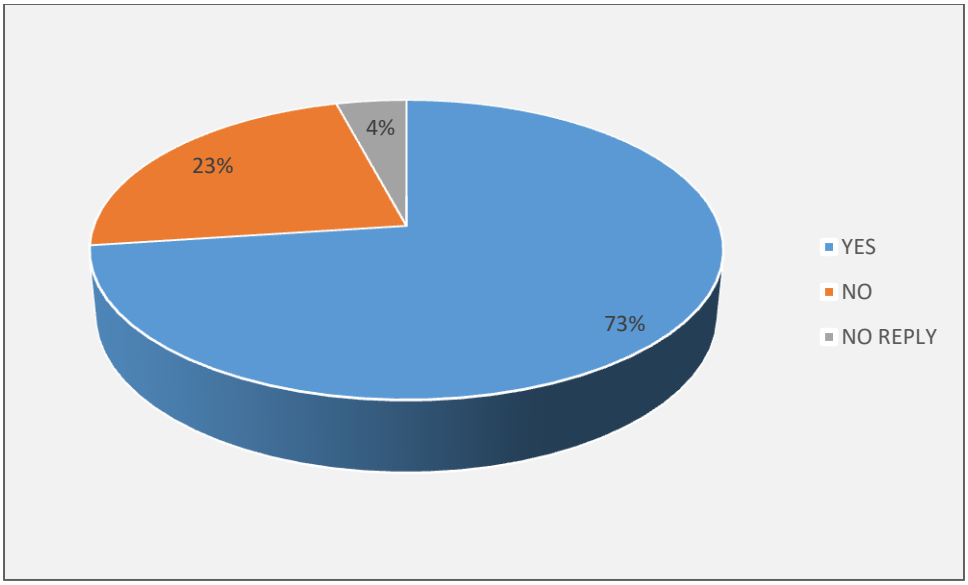

Figure 19: Distribution staff allowed to use personal devices for official business

The research then sought to understand the reasons why the 23% respondents were not allowed to use personally owned devices for official responsibilities. The respondents were asked the reasons why they do not use personally owned devices for official responsibilities at work. Below are some of the reasons they gave:

(i) Organizational policy does not permit the use of personally owned devices
(ii) The nature of the work the respondents were handling
(iii) Possibility of misusing information when accessed from personally owned devices
(iv) Adequate provision of organizational facilities to access computing resources
(v) Information and network security concerns

The majority of respondents were allowed to use personal devices for official business. For the researcher to comprehend the extent of use of BYOD among respondents who responded affirmatively, the respondents were given an opportunity to illustrate their opinion on this matter. They were asked to indicate the extent to which they agreed with three key statements regarding the use of personal devices for official duties.

A significant proportion of the respondents amounting to about 74% did not see any harm in using their personally owned devices to perform official responsibilities at work. 17% chose to be neutral while just 9% did not have an opinion on the use of personally owned devices at work. The majority of the respondents were neutral on using the organization's provided computing resources to perform their work, hence this metric did not provide a good basis for evaluating their satisfaction. It was also noted that most respondents were able to connect to the corporate environment using their devices. The table 3 below shows the summary of the findings on how different respondents expressed their opinions.

No.	Choice/Opinion	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	I don't see any harm in using personal devices (Tablets, Smartphone, Laptops) for work related duties	17%	57%	17%	6%	3%
2	It's okay for me to connect to the office network using the device in the office?	9%	14%	60%	11%	6%
3	I am able to remotely (when out of office) connect to the office network using my device	14%	51%	29%	3%	3%

Table 3: Summary of respondent opinions on use of personal devices for official business

4.3 Summary findings on Prototype Testing

Once the prototype was developed, it was tested for both functional and non-functional requirements to verify whether the research objective was met. The functional testing was done using structured test cases which were derived from the functional requirements outlined during the designing of the prototype. On the other hand, non-functional testing was based on usability metrics as a measure of its readiness for use by different stakeholders. The prototype was stressed against performance, response time, usability, robustness and reliability as the main validation criteria for user interaction.

Questionnaires were provided to each focus group that outlined each test case with a common evaluation framework. The standardized questionnaire template ensured consistency in content across all the users and scenarios. The results obtained from the tests were used to determine the

readiness of the prototype, how it operates in the BYOD environment of an organization as well as the specific behaviour when deployed.

The functional testing of the prototype presented noted that the prototype was able to capture the static data of a user and the device details correctly when inputted by the system administrator. These details were stored on a database. The prototype did not allow incorrect data inputs such as alphanumeric data to be saved on the database where the field required numeric characters only. This was an expectation which was successfully achieved.

The prototype was further tested on its functionality where test cases were designed to verify whether the correct combination of a username, password and MAC address of a correctly registered user and device would grant access to organizational resources as envisaged on the design. It was observed that indeed these parameters had to have the correct combination for access to be granted. The one-time password was also sent to registered mobile numbers for second level authentication whenever the correct username and password is inputted using a registered device.

Error handling was also part of the testing regime that the prototype was subjected to. Whenever there was any failure, it was expected that the prototype would throw an error. It was noted that the prototype would display errors on the instances where the user changes the device without prior advice to the system administrator, input wrong combination of username or password as well as when the one-time password that is inputted is wrong.

While the usability testing gave a clear indication that the prototype was ready for use, different stakeholders rated the different metrics differently. Potential system administrators were asked whether they were able to register new users to access privileged organizational resources, and manipulate static data on the prototype. Since system administrators are technical users, it was recorded that 100% of the users were able to use the system without any difficulty. Therefore, the users found it easy and simple to learn and comprehend the solution without any technical background.

This prototype was developed to process identity and authentication of users and devices in an organization setup where employees were allowed to bring their own devices to work. Efficiency in processing authentication requests by these employees without any delay was a performance and response time measure where respondents confirmed that indeed they were able to access the systems without delay. The entire duration for authentication and validation to allow or disallow access to resources were all within acceptable limits.

The prototype was also tested on how it handled errors during the execution of data inputs. It was expected that any unexpected errors would be handled by the prototype and proper error messages displayed to assist the user troubleshoot. The respondents were asked how robust the prototype was in handling errors. A third of the respondents accounting for 33% rated the prototype to be excellent, 47% said it was very good while 13% rated the prototype as good. A minority of 7% rated it as fair. Since this was an iterative process, there were cases where the system would fail and those failures contributed to majority of the 7%.

Table 4 below is a summary of the non-functional testing on the prototype that was conducted using structured questionnaires that were answered by 15 respondents.

	Simple	Moderate	Somewhat complex	Complex	TOTAL
Performance	67%	27%	7%	0%	100%
	Excellent	Very Good	Good	Fair	
Response Time	80%	13%	7%	0%	100%
	Strongly Agree	Agree	Neutral	Disagree	
Usability	40%	53%	7%	0%	100%
	Excellent	Very Good	Good	Fair	
Robustness	33%	47%	13%	7%	100%
	Accepted	Not sure	Unacceptable		
Reliability	60%	27%	13%		100%

Table 4: Summary of non-functional testing results

CHAPTER FIVE: CONCLUSION

Information and network security is a major concern in organizations especially in the wake of rampant cybercrime. Many organizations that have already adopted BYOD technology have had to change their information security architecture so as to accommodate technological advancements with minimum cost implications. This section mirrors findings of the research in relation to its objectives and presents the deductions that the researcher was able to make. It provides a summary of an analysis of the proposed prototype in answering the research questions.

5.1 Conclusions

5.2.1 Review existing BYOD models

The research study set out to address illegitimate access to organizations' systems via the use of legitimate devices and applications by unauthorized users. An empirical review of significant past studies done on BYOD adoption models demonstrated the need of coming up with an integrated solution that would seek to combine device identification and user authentication into an augmented model which would guarantee in-depth security in the BYOD environment. Four different BYOD adoption models were reviewed with each presenting different limitations that ranged from the choice of device to the complexity and cost of the model in implementation. However, these implementation models provided a basis through which the research formulated the identity and authentication model for bring your own device in organizations. The prototype model in this research was an enhancement of the existing implementation models.

5.2.2 Factors that influences device identity management and user authentication

There are different factors that influence device identity management and user authentication for BYOD in organizations. The extent of the adoption of BYOD in organizations was noted to be marginally low due to a number of reasons that were noted to centre on information security and privacy concerns. However, the study revealed that adoption of BYOD enabled employees to become more responsible in resource utilization, which translated to increased mobility, higher job satisfaction, and greater efficiency and productivity. While the research did not measure these factors empirically, it was noted that respondents from organizations that allowed the employees to use their personally owned devices for work use created some level of satisfaction on the user. This, therefore, means a model for the implementation of BYOD in organizations is essential to the extent that the organization is able to reduce capital expenditure on devices and safeguard its data against unauthorized access, while at the same time encouraging work flexibility and minimizing responsibility for device maintenance and management.

5.2.3 Development and testing of an integrated model

The development and testing of the prototype was conducted in a controlled environment which could be replicated in large scale production environment to serve as a proof of concept and a means of experimentation. The prototype testing validated that indeed this would be an augmented solution for identifying devices as well as authenticating legitimate users to access organization resources.

5.2 Contribution of the research

The concept of BYOD has enabled employees to transition between business and personal tasks seamlessly, hence encouraging them to work using their own devices. While employees enjoy the freedom the BYOD scheme offers, the convenience of BYOD has also raised significant data security risks which should be addressed to ensure adoption of this model is achieved.

The development and testing of the prototype that could offer organizations assurance over the security of their data and address privacy concerns while incorporating the concept of BYOD serves as a significant contribution of this research to the body of knowledge. However, the practicality of the prototype can only be realized and enjoyed when it is fully adopted and implemented by organizations.

5.3 Suggestion for future research

A successful organizational transformation in the wake of digital disruption has necessitated organizations to adopt foreign concepts such as BYOD in order to remain competitive. The research study concluded that most organizations have remained uncomfortable with allowing their employees to use their own mobile devices to access organizational systems. There was a gap in ensuring efficiency, flexibility and quick response times by employees while at the same time protecting the privacy and confidentiality of the organization's private data. Therefore, this research recommends an empirical study on factors affecting adoption of BYOD in organization.

REFERENCES

Aberdeen Group, 2012. Endpoint Security and Endpoint Management in the Era of Enterprise Mobility and BYOD: Still Better Together. *An Aberdeen Group Whitepaper*

Alberta Education, 2012. *Bring Your Own Device: A guide for schools*. [online] Government of Alberta. Available at: <http://www.education.alberta.ca/media/6724519/byod%20guide%20final.pdf> [Accessed 31 March 2019].

Brandly, T., 2011. *Pros and cons of Bringing Your Own Device to work*. [online] PC World. Available at: <http://www.pcworld.com/businesscenter/article/246760/pros_and_cons_of_bringing_your_own_device_to_work.html> [Accessed 12 March 2019].

Ernst and Young, 2013. *Bring Your Own Device: Security and risk considerations for your mobile device program.* [online] Ernst and Young. Available at <https://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/%24FILE/Bring_your_own_device.pdf> [Accessed 12 March 2019].

Evans, D., Gruba, P., and Zobel, J., 2014. *How to write a better thesis*. New York: Springer International Publishing.

ISACA, 2011. *2011 ISACA Shopping on the job survey: Online holiday shopping and BYOD security—Asia.* Schaumburg, IL: ISACA.

Jie. W, Arshad, Junaid and Sinnott, Richard and Townend, Paul and Lei, Zhou. (2011). A Review of Grid Authentication and Authorization Technologies and Support for Federated Access Control. ACM Computing Survey.

Mwenemeru, H. K., 2013. *A model to guide in the adoption of bring your own device concept in an organization*. Strathmore University. Available at: < https://su-plus.strathmore.edu/handle/11071/2342> [Accessed 27.02.2019].

Otenko, A., Chadwick, D.W. and Ball, E., 2003. Role-Based Access Control with X.509 Attribute Certificates. *IEEE Internet Computing*, 7(2), pp.62-69.

Peersman, G., 2014. *Overview: data collection and analysis methods in impact evaluation*. Florence: UNICEF Office of Research - Innocenti.

Thompson, M. R., Abdelilah, E., and Srilekha, M., 2003. Certificate-based Authorization Policy in a PKI Environment. *ACM Transactions on Information and System Security*, 6(4), pp.566–588.

Voas, J., Miller, K.W. and Hurlburt, G.F., 2012. BYOD: Security and privacy considerations. *IT Professional*, 14(5), pp.53-55.

Willis, D., 2012. *Bring Your Own Device: New Opportunities, New Challenges*. [online] Available at: <https://www.gartner.com/doc/2125515/bring-device-newopportunities-new> [Accessed 10 March 2019].