2017

Identity management and user authentication approach for the implementation of bring your own device in organizations

Ray Odero Ouko
Faculty of Information Technology (FIT)
Strathmore University

Identity Management and User Authentication Approach for the Implementation of Bring Your Own Device in Organizations

Ouko Ray Odero

Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Information Technology (MSc.IT) at Strathmore University

Faculty of Information Technology

Strathmore University

Nairobi, Kenya

June, 2017

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

OUKO RAY ODERO…….. **[Name of Candidate]**

…….. **[Signature]**

……..…….… **[Date]**

Approval

The Thesis of **Ouko Ray Odero** was reviewed and approved by the following:

Dr. Humphrey Njogu,

Senior Lecturer, Faculty of Information Technology,

Strathmore University.

Dr. Joseph Orero,

Dean, Faculty of Information Technology,

Strathmore University.

Professor Ruth Kiraka,

Dean, School of Graduate Studies,

Strathmore University.

Abstract

Recent years have seen gradual and systematic acquisition of devices by individuals and using of them as both personal and corporate devices. With the rapid development of new technological enhancements, there has been a shift in the way organizations and employees carry out their business. It is this rapid change from the traditional way of doing office work and/or business that has necessitated the adoption of new practices such as BYOD. To this effect then, corporates are faced with new security and privacy challenges in today's mobile environment one among many being Identification, Authentication, Authorization and Access Control of the users. The research aimed to delve into the factors such as Mobile Device Security Models and Architectures, and current solutions that are being implemented when adopting BYOD whilst considering their strengths and weakness. This analysis of strengths and weakness is what showed that the current solutions are mainly device, data and/or application-centric and have not taken into consideration that illegitimate access to corporate systems can be made via the use of legitimate device and application by unauthorized users. The proposed device identity and user authentication management system is a strong hybrid of the device identity and user authentication solutions that sought to have an augmented solution there by having security in depth in the BYOD environment. The solution used the combination of the unique Media Access Control address and the device owners' personal phone numbers which were concatenated for identification and authentication of the user device and its respective owner whereas an access control register was used for access authorization thereafter. The test results were discussed elaborately for clarity and to give merit for the need of this research work. The prototype tests were based on functional and non-functional requirements of the system. Sampling of the eventual testing results shows an average of 72.8% acceptability margin and potential of quick adoption among users which indicated a positive response to the implementation of the solution.

Key words: Mobile Device Management, Mobile Application Management, Mobile Information Management, Mobile Identity and Access Management, Bring Your Own Device.

Acknowledgements

I am highly grateful to the Almighty God for all His love, kindness, guidance, knowledge and wisdom.

I owe much gratitude to my supervisor; Dr. Humphrey Njogu for the exemplary role he played in guiding me through this entire thesis writing period. Thank you for your invaluable advice, guidance, feedback and patience throughout my research writing process.

I would also like to acknowledge my Master of Science in Information Technology colleagues for their academic and moral support.

Dedication

This thesis is dedicated to the Almighty God for the sufficient grace, strength and good health throughout the two years of my Master's degree program. To my Father Dr. Vincent Ouko Agai, Mother, Eng. Rose A. Wanga, my brothers Eng., MSc., MBA. Ouko J. Onyango, Dr. Ouko M. Hurbart., Eng. Ouko S. Allen and Ouko Ezra thank you all for being a strong pillar in my life.

Abbreviations / Acronyms

BYOD - Bring Your Own Device

BYOT - Bring Your Own Technology

EMM - Enterprise Mobile Management

IAM - Identity and Authentication Management

IT - Information Technology

MAC - Media Access Control

MAM - Mobile Application Management

MCM - Mobile Content Management

MDM - Mobile Device Management

PC - Personal Computer

SSO - Single Sign On

Definition of Terms

Bring Your Own Device (BYOD): A term used to refer to the trend of bringing a personally owned mobile device to the workplace for use and connectivity on an Institutional network (International Data Corporation, 2011).

Mobile Device Management (MDM): Software designed to securely manage mobile Devices used across an enterprise (Trend Micro Incorporated, 2012).

Mobile Application Management (MAM): A system used by IT administrators to remotely install, update, remove, audit, and monitor enterprise related applications on mobile devices (Eslahi & Var, 2013).

Mobile Content Management (MCM): A system designed to secure critical enterprise information by preserving it in a centric location and securely share it between different endpoints and platforms (Eslahi & Var, 2013).

Mobile Device: A handheld computing device that can be used from multiple locations; Examples include basic phones, portable media players, and Smartphone (Crisp & Williams, 2009).

Smartphone: A fully-featured mobile telephone with personal computer-like Functionalities (Green, 2007).

Consumerization of IT: The cycle of information technology (IT) emerging in the consumer market, then spreading to business and government organizations, largely because employees are using the popular "consumer market" technologies and devices at home and then introducing them in the workplace (Trend Micro Incorporated, 2012).

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Background of the Study

The rapid technological growth and development is fast changing the traditional habits of individuals and how they carry out their daily business. These changing of habits represent an opportunity and a challenge for the enterprises. The opportunity is related to two main aspects: the productivity increase and the costs reduction. In a BYOD scenario, the end users would pay totally or partially for the devices and would work independently from time and location. On the opposite side, the new scenario brings some risks that could be critical. The use of devices for both personal and working activities opens to new security threats to face for IT organization (Scarfo, 2012).

The features of portable devices that make them handy, convenient and enable them to have a real time connection to various networks and hosts also make them vulnerable to losses of physical control and network security breaches (Ernst & Young, 2013). Clearly, there are several important advantages for employees and employers when employees bring their own devices to work. But there are also significant concerns about security and privacy that relate to data confidentiality, user authentication and access authorization. Companies and individuals involved, or thinking about getting involved with BYOD should think carefully about the risks as well as the rewards (Miller, Voas, & Hurlburt, 2012).

BYOD trend gives a unique opportunity for fast growing futuristic companies to harness this collective power to their advantage. Along with these benefits, however, this trend also gives rise to new challenges related to visibility, data access, and data protection that require organizations to reassess their existing security and management strategy (Crook, 2011). From the onset, it is clear this is both a blessing and curse depending on the point of view you want to look at it.

The BYOD/mobile environment has fundamentally changed the organization security topology and introduced a set of new rules i.e.:

(i) Mobile device usage is redefining organizational security requirements.

Despite the significant advantages of the BYOD model, the concept introduces new security challenges; for instance, the organization loses the ownership of devices used for official work, to the employees. Implying that the employees own and manage the devices they use to work, including seeing to the security needs of such devices. With this development, protecting the corporate network becomes pertinent and even more challenging with an audacious need for outwitting conventional access control mechanisms, giving the highly dynamic nature of mobile devices. For the general IT supportability of BYOD environments, new security measures such as Information management policies should be put in place and strictly complied with.

(ii) The gateway is no longer the main point of control.

With personal devices now being used to access corporate applications and data, many organizations are struggling with how to fully define the impact to their security posture. To mitigate the breach in security, IT environments are opting to have many/different points of control. For instance; some BYOD environments prefer to have the data stored centrally so as to regulate its access with device specific identifiers e.g. MAC addresses, use of dynamic access control technology based on context information. While others reason that authentication is both user and device based, they prefer to have biometric applications installed on the mobile devices. This in the current state of the Kenyan organizations cannot be achieved currently and more so for the purposes of the research. Therefore, MAC addresses and passcode are the most feasible ways to achieve the research objective.

(iii) The new security perimeter is users, devices, and data.

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. However, the security concern is shifted to who and what can access an enterprise's wealth of data. Identity theft, data leakage, distributed denial of service (DDoS), and malware are the most challenging security threats in BYOD (Morrow, 2012). There are several causes of these threats; these could range from malicious user of the mobile device, remote

access of the device by an attacker, loss of the mobile device to use of Trojan applications by an attacker and so on.

Due to this, organizations find themselves in a situation where the external demands push them towards accepting the changes in the technology space in order to remain competitive and in business and on the other hand the internal demands bring to question how are the system and security administrators enabled to enforce network security policies to allow access and privileges and remain secure and protected from being intruded through the same technology that determine whether or not they remain in business depending on the severity of the intrusion.

Therefore, the frameworks upon which the solutions are implemented on must incorporate controls around people (users), corporate processes, and all of the technology (devices) that access corporate resources.

Existing BYOD solutions are not able to handle the challenge of uniquely identifying a user device and its legitimate user and the research work sought to look at a number of solutions and their strengths and limitation and propose a new approach that will provide a more secure and advanced solution to organizations.

1.2 Problem Statement

As companies adopt smartphones for their businesses, the Bring-Your-Own-Device concept is raising many security and privacy concerns for administrators and IT professional (Burt, 2011). With the inherent need of organizations to continually change with modern technological, portability and flexibility advancements in order to remain competitive, it is imperative that they adapt and figure out new ways to accommodate (adopt) these new technologies and practices.

Several research efforts have been undertaken to ensure that devices, applications and content/information remain secured to enable businesses operate in secure and safe environment bearing in mind the vulnerabilities and numerous threat vectors that organizations are predisposed to. The existing solutions do not adequately address the issues of identity management and user authentication creates a security gap that ought to be filled. Even with secure devices, applications and content there exists the threat of identity theft which may result

into a breach of the entire network infrastructure. It is, therefore, incumbent upon organizations to ensure that they can authoritatively confirm the identity of a user before they can allow them to have access to sensitive data and information via their network and that their privacy and security is not compromised.

Based on the aforementioned challenges, the solution being proposed will incorporate a comprehensive Mobile Identity and User Authentication Management system to the already existing Enterprise Mobile Management model through the capture of the unique device identifier (MAC) address that is associated to the primary phone number of the device owner in a central database and generation of a one-time random code.

1.3 Research Objectives

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

(ii) To identify factors that influences the mobile identity management and user authentication for BYOD devices.

(iii) To build a strong integrated identity management and user authentication solution for organizations.

(iv) To test the proposed Bring Your Own Device identity management and user authentication solution.

1.4 Research Questions

(i) What are the strengths and gaps of the existing solutions?

(ii) What are the factors that influence the mobile identity management and user authentication for BYOD devices?

(iii) How can a solution that takes care of identity management and user authentication for BYOD be developed?

(iv) How can the proposed BYOD solution be tested?

1.5 Justification

BYOD faces a myriad of security and privacy challenges both in its adoption and implementation. There have been continuous advancements in this area of research and tremendous efforts undertaken to shed light on the topic at hand. However, the research approach was on how to adopt and implement an integrated and robust BYOD model that will aid in the identity management and user authentication in organizations. As such, the research ensured that the appropriate coverage was expansive enough to meet the globally acceptable practices but locally deployed.

In light of this, the research paper, therefore, offered to propose a better model that will fill the security gaps which will in turn enable organizations accept the emerging trend of BYOD/BYOT and remain secure in their corporate network.

1.6 Scope of Research

The primary focus of the research is to propose identity management and user authentication solution that will help organizations achieve a full identity spectrum i.e. Authentication, Authorization and Access Control.

1.7 Limitation of Research

According to Best & Kahn (1998), limitations are conditions beyond the control of the researcher that may place restriction on the conclusions of the study and their applications to other situations.

The main limitation of the research was how to be able to select institutions and individuals who were to be used as focus groups for the software iteration tests. These groups were to provide a good representation of the other organizations.

Chapter 2: Literature Review

2.1 Introduction

This chapter sought to present a background on the past and current adoption and implementation strategies of BYOD necessary to establish the context of this research study. The chapter explores academically and industry tested models and solutions with a view to understand the network security and privacy issues surrounding the BYOD concept. The literature is reviewed along three themes; Understanding BYOD as a concept, Empirical review of significant past studies on the BYOD Benefits to the Organization, BYOD Security Risks and Threats to the Organization, BYOD Security and Privacy Issues and Mobile Device Security Considerations.

2.2 BYOD Concept

According to Brandly (2011), BYOD is a process where the organization's management decides to allow its employees to use personally owned devices such as laptops, mobile phones among many others for work purposes. The trend of Bring Your Own Device (BYOD) is creating a new change related to enterprise IT in many organizations. The exponential increase of consumer device market from 2009 – 2015 has seen growth of new mobile devices with features comparable to those provided by PC workstations. A survey by ISACA, (2012) suggests that 54% of employees have a personal device they use for work. Its therefore evident that BYOD is causing a shift in the use of consumer IT by employees to achieve their work activities.

Table 2.1: Consumerization of IT of Trends (Krishnan, 2011).

End User Trends **Question: How do you manage this change?**	
Then: PC Era	Now: Post PC Era
Traditional desktop form factors (laptops, desktops)	Compact and mobile devices (smartphones, tablets) share galloping
Largely location defined workforce	Distributed, decentralized and mobile workforce
Clear distinction between business-owned and personal devices	Line between business and personal devices blurring; employee owned devices being used for business
One organization – one platform; standardization	One organization – many platforms; flexibility

Enterprise innovation is a catalyst for business growth but with these innovations, enterprise information security poses a challenge which may hinder the adoption of innovations such as Bring Your Own Device (BYOD). The nature of today's businesses is its ever changing and agile and as such the approach to information security should be pragmatic. Efforts have been made to implement strict security requirements as an overlay to a perimeter-focused network and device-centric security models but still fail to adequately secure enterprise data, failing the agile enterprise. Ernst & Young (2013) conclude that the features of portable devices that make them handy, convenient and enable them to have a real-time connection to various networks and hosts also make them vulnerable to losses of physical control and network security breaches.

2.3 BYOD Concept Adoption in Organizations

The BYOD concept covers the following key areas namely Device, Applications, and Information /Content. With the advancements in technology organizations are forced to embrace consumerization of IT which increases their risk exposure. Even so, they do their risk assessment and put in the necessary counter measures to mitigate the risks. In addition, organizations that allow employees to work with the technology they are most comfortable with tend to have more satisfied employees while also enjoying the addition advantage of cost savings (Crook, 2011).

Botha, Furnell, & Clarke (2009) point out that portable device security has become a point of neglect by most organizations. As companies adopt smartphones for their businesses, the Bring-Your-Own-Device concept is raising many security concerns for administrators and IT professional (Burt, 2011). Although this concept lets employees easily use their own devices to access corporate applications and resources and realize invaluable business benefits, enforcing security policies on a personal device is difficult (McAfee, 2011). To maximize on the benefits of BYOD adoption and implementation while ensuring secure corporate informational assets, certain key security considerations have to be looked at.

The main goal of this Empirical review was to be able to identify the gaps in other studies and provide the relevant solutions to fill in the gaps.

2.3.1 BYOD Benefits to the Organization

According to Sen, (2012) on the consumerization of IT drivers, benefits and challenges for the New Zealand Corporate a number benefits realized due to adoption of the bring your own devices concept included but may not be limited to an acceleration of business growth, increased productivity in the organization due to employees bringing in new technology, employee productivity through trust, and provision of cost benefits to the organization. These benefits when looked from a business strategic point, they improve operational efficiency and effectiveness thereby making the business have a competitive edge by being more agile and profitable.

2.4 BYOD Adoption Challenges to the Organizations

Numerous challenges such as securing the data, ensuring the quality of the service and setting the policies to determine the level of access the devices have to the network are but a few posed in the work environment by the personally owned devices (Burt, 2011). It is therefore clear that even though we realize a myriad of benefits through BYOD, the challenges are now more than before ever present and cannot be overlooked. They include:

(i) Enabling users to securely accomplish work-related tasks on personally owned devices.

(ii) Accommodating a diverse inventory of mobile devices.

(iii) Effectively enforcing policies for both personally owned and corporate-provisioned devices, and enforcing different policies for different user types.

(iv) Minimizing the administrative burden of BYOD on staff.

(v) Supporting all aspects of the mobility landscape.

(vi) Controlling the organizations' content to ensure confidentiality of the data.

(vii) Varying complexity of some devices in terms of their configuration and specifications may lead to loss of time.

2.5 Factors that influence the mobile identity management and user authentication for BYOD devices

With the BYOD security perimeter mainly encompassing the user, device and data, serious security concerns rise in terms of Confidentiality, Integrity and Availability. Data confidentiality entails the protection of sensitive information from unauthorized users. Data integrity encompasses changes to the data and the identification of the individual or system that changed it. Availability is whether or not the data can be accessed by users or systems when required.

In BYOD deployment, it is imperative that firms put measures to mitigate risks that may arise from the three. These measures are influenced by a couple of factors such as Privacy, Data Protection and Variations of the Mobile devices. A sound and easy-to -comply with Privacy policy surrounding personal mobile devices should be put in place. Otherwise it could be hard to hold an employee liable to a breach of such policies especially if device is the sole ownership of the employee or in another case where the employee is not aware the implications of a breach in the privacy policy.

Data protection encompasses both personal information and enterprise data. Employees want to feel that their personal information is in no way entangled with the organization's data and that their privacy is upheld. In the same way, the employer wants the organization's wealth of data protected from unauthorized persons. Due to the large variations of personal devices, platforms, operating systems, etc. it is hard to implement clear-cutting security measures. For instance, in a scenario where an organization uses biometric form of authentication, it would spend more money to come up with a harmonized way for all the different mobile devices to run

on a particular biometric application. It is these factors such as cost-benefit analysis that necessitate the need to have a cost effective and efficient solution to deal with identity and authentication security concerns.

The figure 2.1 gives a summarization of four top security concerns in addition to the above-mentioned challenges:

Figure 2.1: Top Concerns of BYOD are related to security (Forrester, 2012).

It is also important to note that BYOD privacy and ethical issues have legal implications. Organizations should be aware of the evasive nature of security measures they put as risk management mitigation strategies for the employee devices and how they comply with data privacy rights and regulations. Personal identifying information should be kept private and confidential and avoid any leaks and/or unauthorized access due to their sensitivity. Failure to which may lead to lawsuits. Globally acceptable data privacy laws require mandatory consent of the employee before companies install invasive security measures or access data on personal devices for the company to provide adequate protection. Good security solutions should be proactive and remain transparent to the system user in any environment i.e. do not restrict how employees interact with devices outside of work.

2.6 Mobile Device Security Considerations

The BYOD concept should be viewed in a broader perspective due to its complexity and hidden implications not just shifting ownership of the device to the employee. This will ensure a more robust and informed strategy in its adoption and implementation. As a result, there are components which may be considered by organizations in adopting BYOD and they include:

(i) Device choice.

(ii) User experience and privacy.

(iii) Trust model.

(iv) Application design and governance.

(v) Liability, economics, sustainability and internal marketing.

Companies that wish to adopt BYOD ought to prepare themselves to meet costs, either of purchasing and/or supporting the installation of various features that may be needed in the personal devices.

International Data Corporation in its report on consumerization of IT included several key components for consideration by any organization to support the successful adoption of BYOD and applications in the workplace. Some of the components are:

(i) Establishment of revamp policies.

(ii) Investing in technologies and services that allow security on personally-owned devices within and outside the workplace environment.

(iii) Developing better visibility into an organization's adoption of consumer-rooted devices and applications and engaging the organization's executives.

2.7 Existing Mobile Device Security Models and Architectures

The models of BYOD adoption differ from one level of needs to another (Alberta Education, 2012). Among the models of BYOD adoption is the Integrated model which considers a range of acceptable devices and categorizes in a spectrum ranging from high standardization to high flexibility. As shown in figure 2.3 below, standardization is the identification of a single type of device that all device-owners must purchase on one end whereas flexibility is an open-ended model that encourages the device owners to bring with them any device on the other end. According to Alberta Education (2012), integrated model combines a number of aspects: limiting the devices to a specific brand or model, limiting the devices to those that meet specific technical specifications, limiting the devices to those with specific functionality and devices that are Internet-ready. Figure 2.2 illustrates an integrated model of BYOD with a range of acceptable devices which fall onto the spectrum from high standardization where only specific brands and models of personal devices are accepted by the organization to high flexibility in BYOD adoption. The models include mobile device management and mobile application management.

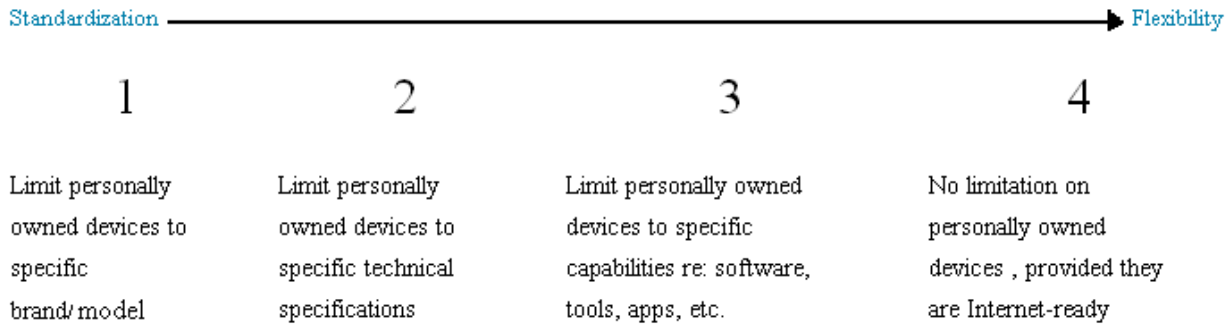


Figure 2.2: Classification of BYOD Models from the Least to the Most Flexible (Alberta Education, 2012)

2.7.1 Akenti

Abdelilah, Srilekha, & Thompson (2003), propose a certificate-based authorization policy in a PKI environment known as Akenti. In their work Akenti aims to deliver scalable security services in highly distributed network environments. Akenti achieves this through the management of authentication and authorization issues. In addition, the whole access control is managed through the use of a number certificates and access decision from the provider are given in a very strict way. The advantage of this is it allows a simple structure and easy transmission of data. The verification of acceptable issuer signature, evaluation and access authorization is done by the Akenti server.

However, Akenti authorization model has the following short comings; all policy certificates are stored at a central point and therefore new service providers who wish to join are not quickly integrated especially in large communities. Also, identity is directly linked with permissions and as such may be vulnerable to fragmentation and inconsistencies between the permissions. The Akenti certificates do not conform to the standard.

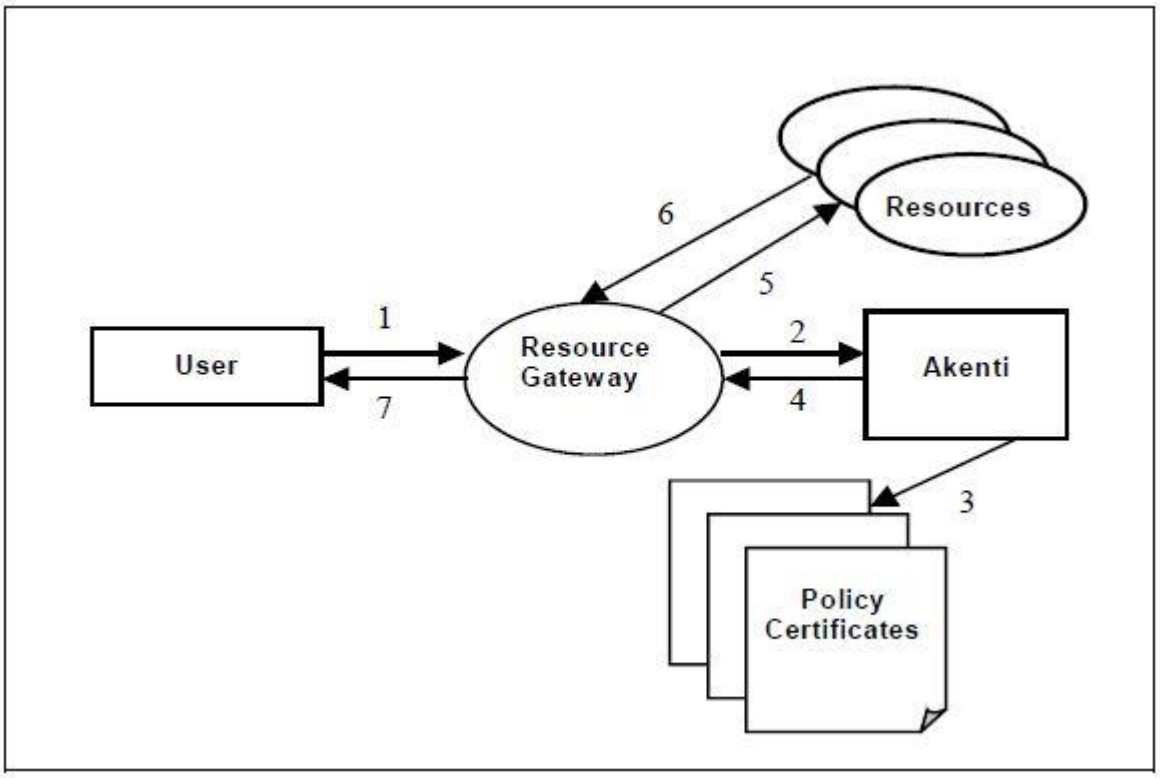


Figure 2.3: Akenti Authorization Model (Abdelilah et al., 2003)

2.7.2 Privilege and Role Management Infrastructure Standards Validation (PERMIS)

According to Chadwick et al., (2008), the PERMIS authorization infrastructure provides facilities for policy management, credential management, credential validation, and access control decision-making. Users make requests which are intercepted by applications which ask PERMIS to validate the user's credentials and make an access control decision. Ones validated PERMIS enforces the access control decisions and obligations and gives a return/response. PERMIS is attribute certificate based authorization and the certificates contain the specific user roles. PERMIS cannot be seen as a feasible Identity management and user authentication management system because the process of handling attribute certificates is complex in nature and storage is in a central repository which results in the lack of a high information granularity as presented by the user. This raises privacy issues and the resource provider is forced to send defined policies to the repository. The figure 2.4 depicts the architecture of the PERMIS authorization infrastructure:

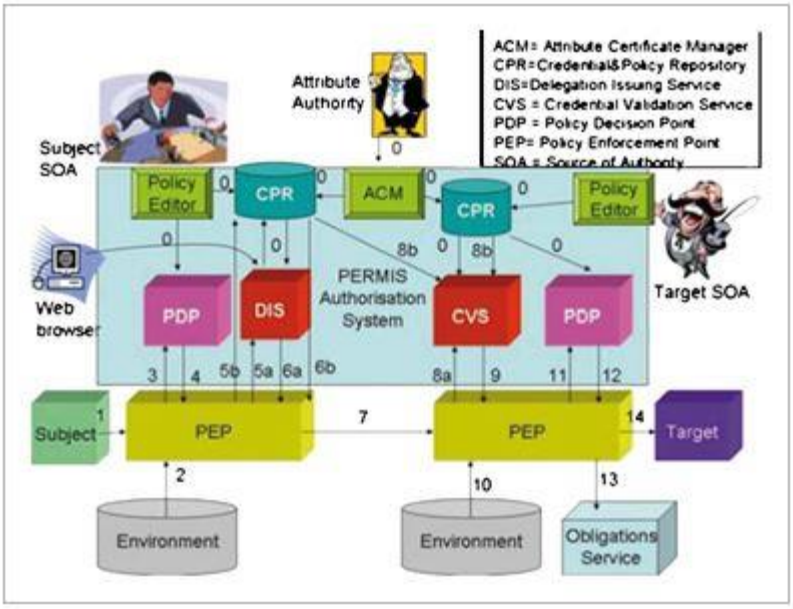


Figure 2.4: Architecture of the PERMIS authorization infrastructure (Chadwick et al., 2008)

2.7.3 Community Authorization Service (CAS)

According to Pearlman et al., (2002) building on the Globus ToolkitTM Grid Security Infrastructure (GSI), Community Authorization Service (CAS) allows resource providers to specify course-grained access control policies in terms of communities as a whole, delegating fine grained access control policy management to the community itself. CAS identity model offers a simplistic approach that does not record groups or roles. The used information is stored in a critical section of the transmitted certificates so that those servers that are not aware of the CAS system need to be modified in order to work in a federation that uses CAS. The disadvantage of CAS model is the amount of data that is to be relayed is huge making it not convenient as a solution for mobile environments.

2.7.4 Data-centric Information Security Model for Bring Your-Own-Device Environment

According to Juma (2014), Data-centric security model is introduced in the context of a layered security approach for end-to-end security. His focus is on ensuring data security and the overall enterprise architecture by focusing on the key steps of data security with the following key requirements; data classification, applications, roles, users and policies definition. The advantage of his proposed model is it allows organizations a middle ground while adopting Bring-Your-Own-Device concept by ensuring information security without compromising employee privacy demands. To ensure the organizations data is transferred securely across the agile environment, Juma (2014) implements features such as data encryption, audit, digital rights management, and secure file transfer and policy enforcement. The weakness of this approach is that those who access and transfer this data need to be positively identified and authenticated before they are given access rights and/or authorization.

2.7.5 A Model to Guide in the Adoption of Bring Your Own Device concept in an Organization

Mwenemeru (2013), in his thesis "A model to guide in the adoption of BYOD" goes ahead to propose a Hybrid BYOD Model to answer to the key concerns on the adoption of BYOD concept by an organization. To support his idea he says, there are no studies that have been carried out on the integration of own devices in the organizational infrastructure and especially with companies in the Kenyan context (Mwenemeru, 2013). Whereas the integration of own devices with organization's infrastructure will seek to tap into the strengths of the respective BYOD solutions while compensating for each other's weakness, the downside is that the proposed study focused on components such as user privacy, sustainability, device choice, affordability/economics, training consideration, technical consideration, liability and content and overlooked user identity theft and the appropriate authentication mechanisms that can mitigate this which is equally a major security challenge in the BYOD agile environment.

2.7.6 A model to enhance information security in the use of the BYOD in Kenyan enterprises

Ndwiga (2015) proposes a hybrid model to fill the gaps that have been left by previous models. In his approach, he identifies a number of security challenges and narrows down to three top challenges; mobile devices security, mobile information security and mobile applications security. Interestingly, Ndwiga (2015) analyses his results and observes that most of the technical and non-technical measures in place such as firewalls and user awareness or training and mobile device security policy respectively are not specific to mobile device use at the work place and therefore concludes they are not effective in dealing with security issues related to the adoption of BYOD.

2.8 Existing Mobile Device Security Solutions

Allam et al., (2011) have tried to explore different solutions which organizations can implement to assist in the adoption of BYOD concept without increasing their risk exposure level. A forecast on the use of these security solutions below gives a clear view of where the industry is most focused in and safe to say least focused in currently.

Figure 2.5: Global BYOD Security Market (Integrated Solutions, 2013).

2.8.1 Mobile Device Management

According to Gartner (2011), the Mobile Device Management space is just getting under way, though there are already more than 60 vendors in this market. Gartner estimates that in the next three years, revenue in the MDM space will grow 15 to 20 percent; from $150 million in 2010. This popularity is as a result of its ability to cover multiple security threats posed by BYOD. MDM systems remotely monitor the status of mobile devices in order to control their functions. Some of the functions of MDM are; PIN enforcement, data encryption, data wipe, data loss prevention, root detections and application tunnels. The figure 2.6 gives the general MDM architecture and its workings:

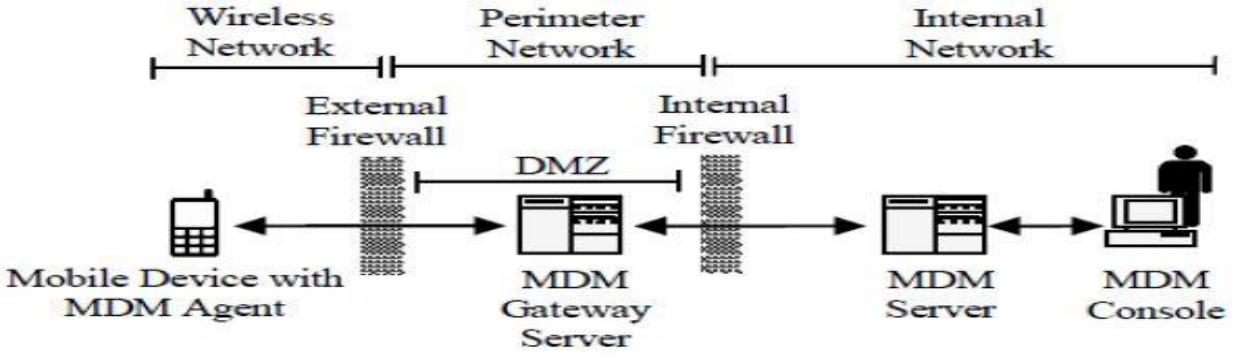


Figure 2.6: General MDM Architecture (Eslahi et al., 2013)

2.8.2 Mobile Application Management

A Citrix study forecasts that by mid-2013, 94% of companies will have a BYOD policy. Gartner adds that by 2014, 90% of organizations will support corporate applications on devices owned by workers. MAM is a flexible alternative to MDM, as the scope of protection concerns a specific set of applications on the mobile device. MAM allows the company to apply security policies, lock down, define access control rules, configure software behaviours, remote wipe applications under its control, restrict access to unauthorized applications and install approved applications. Applications outside of MAM's boundaries remain private and continue to function at the employee's discretion MAM is enhanced when combined with containerization.

2.8.3 Mobile Content Management

MCM also known as Mobile Information Management, is primarily concerned with data integrity and encryption, determines application and personnel access and ensures document synchronization amongst multiple devices, whilst simultaneously administering security procedures such as malware scanning. Company data is located in one place, such as a cloud server, yet is accessed according to permission rules applied to the requesting devices and applications. MCM synchronizes data across devices similarly to cloud storage services; as data is stored in a virtual central location.

2.9 Literature Review Summary

The above security solutions; mobile device management, mobile application management, and mobile information (content) management provide the three fundamental information security goals; Confidentiality, Integrity and Availability. The research appreciates that these are positive steps towards achieving secure BYOD implementation but on the flip side we need to ask ourselves how do we manage user identity and authentication together with access control to corporate applications and other resources. As shown in the Figure 2.5, Mobile Identity Management is the least by percentage in its adoption as a security solution in the mobile environment. The assumed mobile environment consists of different interacting entities, that is, people, processes and technology Firstly, there are the people (users) who are nomadic, often moving between access points and domains. They access the network with their mobile terminals (different technologies), connecting to some services and using them. The actions a user must do to access core corporate system and subsequent use should be made as easy as possible. Organizations provision resources to the users, monitor users' actions and logs their use for accountability and audit. The user identity and authentication management solution being proposed will be a combination of both device and user identity mechanisms that are bound within BYODT policy framework. This is the Next Generation Mobile Environment solution towards achieving a secure and reliable Authentication, Authorization and Access control mechanism.

2.10 Conceptual Framework

The Figure 2.7 gives a conceptual framework of what the system does and how the system does its task. The system user who owns the device requests to access the internal organization resources. The user is prompted to first log in using their username and password that were captured during registration by system administrator. The username and password are entered in the text fields provided on the log in window, which are then compared with those that are pre-stored in the User Authentication Repository via the authentication service provided by the verification engine. Once the username, password and MAC address combination have been confirmed to belong to the particular user, the database responds back to the authentication module which then alerts the code generator to generate a one-time random code and sends it to the registered user's mobile phone number. This code is then keyed in the device interface and access to the resources is authorized via the access control register. The access control register determines which organization resources the authenticated user is allowed to access and what they can do. By doing this comprehensive device identification and user authentication procedure, the user can be positively identified and they cannot repudiate that they were not the one behind the device at the time of logging in.

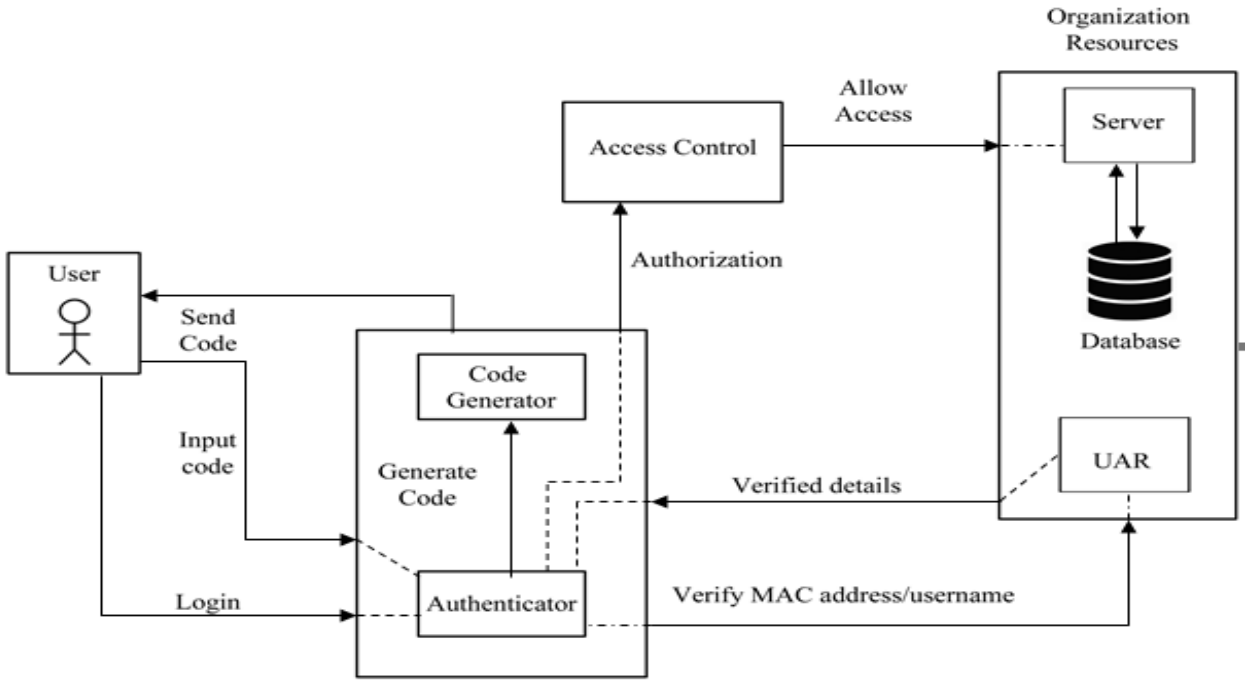


Figure 2.7: A Conceptual Framework of the proposed solution

Chapter 3: Research Methodology

3.1 Introduction

Research methodology is a way to systematically solve the research problem i.e. a scientific study of how research is done scientifically (Kothari, 2004). The methodology that was used in the research aimed at coming up with a new approach of ensuring a comprehensive identity management and user authentication in the mobile environment. The research methodology section was subdivided into subtopics along the following themes: research design, research area, data analysis procedures, software development lifecycle, research quality and ethical considerations.

3.2 The Research Design

Research design is a logical inquiry that enabled the researcher to obtain evidence which was in turn used to answer the initial research question as clearly and precise as possible. The research design used in this study was a mixed research approach.

The intent of this research is to come up with a solution to address mobile device identity and user authentication management. The research design allowed use of various methods of data collection like questionnaire and interview guides as well as the use of standardized questions where reliability of the items was determined (Owens, 2002). To obtain answers to the research questions and achieve the research objectives spelt out in addressing the problem, a mixed method research design was used. According to Cresswell (2003), mixed method research design refers to a procedure for collecting, analyzing and "mixing" both qualitative and quantitative research and methods in a single study to understand the research problem. A number of research types were used during the study, that is, applied research, qualitative research and quantitative research.

According to Kothari (2004), applied research aims at finding a solution for an immediate problem facing a society or an industrial/business organization. The significance of this research will be to look at the fundamental experiences of people while using BYOD in the organizations and understand the various solutions that has been proposed and implemented to ensure secure adoption. As such the functional requirements for the proposed solution will be well deduced.

The applied research was used with the aim of finding a solution for mobile device identity and user authentication problem facing our Kenyan organizations.

A qualitative research ensured that the information collected from both primary and secondary sources during the research were incorporated in coming up with the proposed solution. Cresswell (2003) notes that by doing this then the user requirements are fully satisfied in the developed application and that the deliverables agreed upon are delivered.

The quantitative research was used during the testing phase in the SDLC. This was done through the feedback provided by the users on the suitability of the application's prototype and final product. The testing and feedback cycle was iterative to ensure that the final system meets the user requirements.

3.3 Location of the Study

The research targeted local institutions within Nairobi, Kenya. This is because most of the organization within this area are adopting BYOD which is becoming a game changer and therefore giving the organizations a competitive advantage through innovations such as agency banking. Secondly, because of the limited time provided to conduct the research and financial constraints, Nairobi was picked due to its proximity to the researcher and the fact that agile model was used as the SDLC method it demanded the several iterations were to be done and within shorter time frames. The proposed study looked into how Device Identity, Authentication, Authorization and Access Control protocols are done in the Kenyan institutions.

3.4 Data analysis

Quantitative data analysis approach formed the basis of this research. There are a number of data analysis tools which were used. The data analysis is a core part of the research process as it converts that data in its raw format to a more meaningful data (information). The research used tools such as SPSS for mining the data from the data collection tools. Excel work sheets were also be used for presentation of the data. Excel is good in aiding in clear interpretation of the data due to its simplistic charts and graphical representation of information.

3.5 System Development Life Cycle

The research used Agile SDLC model which combined iterative and incremental process models with focus being on the process adaptability and customer satisfaction through rapid delivery of working software product. The software product was broken down into small incremental builds which were provided to the software users in iterations. Each iteration typically lasted from about one to two weeks. Every iteration involved focus groups selected across functional teams working simultaneously on various areas like planning, requirements analysis, design, coding, unit testing, and acceptance testing.

At the end of the iteration a working product was displayed to the intended system users and important stakeholders. Figure 3.1 shows the agile model phases:

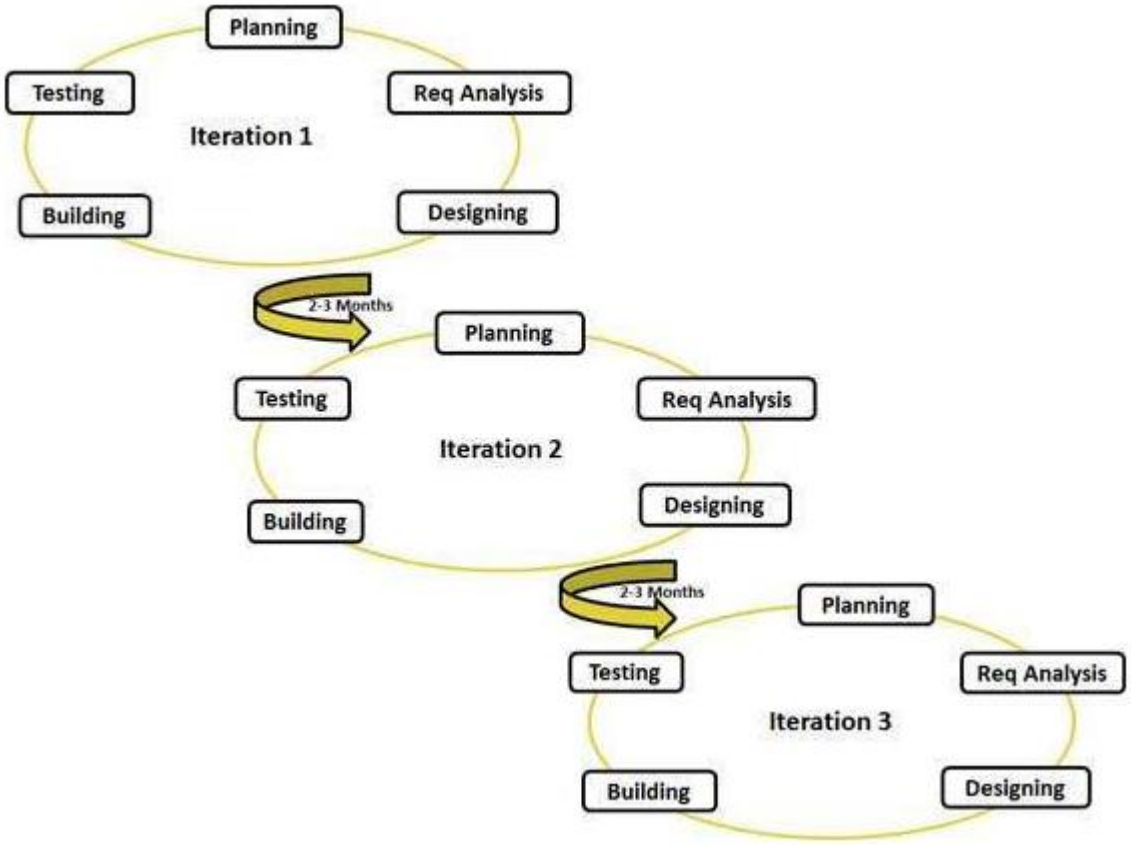


Figure 3.1: SDLC Agile Model (Cockburn, 2002)

The Agile model was best suited for this research because unlike other SDLC models, Agile model believes that every project needs to be handled differently and the existing methods and solutions need to be tailored to best suit the project requirements. The tasks were divided into small time frames to deliver specific features for a release. Iterative approach is taken and working software build is delivered after each iteration. Each build is incremental in terms of features; the final build holds all the features required by the customer.

3.5.1 Requirement Analysis

This is the initial phase of the SDLC and it involved two areas: initial assessment that included the acquisition of requirements which included both system and user requirements of the solution. Secondly, feasibility study was conducted to ascertains whether the inclusion of the device identity and user authentication module into the already existing security infrastructure is something realistic and achievable within the given research conditions. Initial formal and informal interviews were the methods used to collect the requirements for analysis. The outcome of this phase is Requirements Understanding Document (RUD).

3.5.2 Designing

This phase takes from the requirement analysis phase by doing an in-depth analysis of the acquired user requirements. Apart from this, the existing systems are also reviewed and their strengths and weakness critically analyzed. Ones requirements and review of existing systems is done the researcher will be able to link these with the proposed solution intended and the logical system design drawn. The tools used in the design phase will include Entity Relationship Diagrams, Class Diagrams, Data Flow Diagrams, Sequence Diagram and Use Case diagrams. Computer-Aided Software Engineering tools (CASE) are used for implementing these tools. The outcome of this phase is the high-level design document.

3.5.3 Building

During this phase, the proposed system was broken down into granular components. These components are sub-units of the proposed system and they gave a detailed system specification. The outcome of this phase was a detailed low level design document.

3.5.4 Implementation and Testing

In this phase, the solution is in the actual development stage. The tasks that were undertaken in this phase included coding, testing and debugging the system. The dotnet (.net) framework was used in the development of the system and the preferred coding language was vb.net whereas the system's database management system was MySQL. The testing was done inhouse by the developer as well as sending each iteration to the end user. The objective of this phase was to deliver a completely functioning and documented device identity and user authentication system that has been reviewed and approved (Predrag et.al. 2010). Final adoption of the system would include users and performing the actual transition from the old system to the new one and training the users.

3.5.5 Review

The system was reviewed periodically to further improve it. The purpose of the review was for maintenance and enhancements of the solution to correct user identified errors and ensure the system meets the statutory regulatory requirements that may have been overlooked during development. Also, it was to enhance the system performance through optimization.

3.6 Research Quality

The validity of the research design and methodology was reflected by the organizations and focus group selected, the research types, and research instruments that were used. The validity of the research was guaranteed by the use of quality primary and secondary sources of information and the knowledge background of the researcher involved.

The reliability of the sources of information from the sample size, the location of study, the research instruments, and any other concerned research aspect was guaranteed. This was based on the approval of reliable entities in the academic circles such as the supervisor(s), and other sources of knowledgeable information featuring the same methods in previously successful research studies.

3.7 Ethical Considerations

For purpose of adhering to the acceptable ethical standards in the course of the research, the researcher ensured that those who participated in one way or the other to achieve the objectives of the research were assured of their confidentiality. During the research, the researcher sought for the consent of every respondent before any engagement and assured them that the information gathered from them was to be used for the sole purpose of this research and access to the filled questionnaires and focus group interviews was restricted to the research.

Chapter 4: Proposed Model Design and Architecture

4.1 Introduction

System design is a process detailing a given systems' architecture, modules, data and components designed to meet given requirement (Kruchten, 2012)**.** On the other hand, system architecture is a conceptual model that defines the behavior of the system (Kruchten, 2012). This section of the paper will detail the design structure of the proposed solution by incorporating the variously proposed user requirements collected through the various interactions with the potential users and experts. In order to achieve this, design diagrams under the Unified Modelling Language namely use case diagram, data flow diagrams, class diagram and system sequence diagram were used.

4.2 Requirement Analysis

In order to do a proper system design and architecture, the research needed to look at the current models and approaches that have been implemented to guide in the adoption of BYOD within organizations and deduce their strengths and weaknesses. This will ensure a pragmatic approach that is fact based is used to draw conclusion(s) on the system and user requirements and designing of the eventual system being proposed. The outcome of the fact-finding process is software requirements specification (SRS) document which details the functional and non-functional requirements of the system.

To achieve this, we started our system analysis process by collecting data from credible and reliable sources. One of the ways used to obtain the facts about the current solutions being implemented was through interviews. This involved going to the financial institutions i.e. banks and saccos, and having discussions with mainly those tasked with the responsibility of security namely the system administrators, network administrators and the I.T managers. The process involved semi structured interviews that were both formal and informal. Another method employed in our quest to obtain facts was through observation of the normal routine. Here we observed how the staff gained access to the organization resources, using the applications in their personally owned devices and the security controls that were implemented to enforce the security rules. We observed whether those controls were actually working as they are intended to or otherwise. Finally, the researcher obtained facts from reviewing literature from various

researchers who have made a contribution in line with adoption of BYOD in organizations. The outcome of these data collection methods was that the current solutions whereas they ensure devices, information and applications are secure the assumption that those who use them are the intended users is a course of security concern that needs to be addressed. This assumption was found to be a security risk as it was proven that unauthorized person may use a combination of authorized devices and applications to gain access to secure corporate resources. This then poses the question of how do organizations ensure that they can positively identify and positively authenticate the users before granting access to the requested resources.

4.2.1 Functional Requirements

Functional requirements capture the intended behaviour of the system. This behaviour may be expressed as services, tasks or function the system is required to perform (Bredemeyer, 2001)**.**

The following are the functional requirements of the proposed solution:

(i) The system ought to have the capacity to capture details of the device owner, for example, name, telephone number and mac address of the personal device.

(ii) The system ought to have the capacity to securely store the device owner's details at the central database.

(iii) At the point when the user enters the username, the system ought to have the capacity to verify the username, match it with a particular mac address and phone number pre-stored in the database and instruct the code generator to send a code.

(iv) The system ought to have the capacity to generate a one-time random code every time a user requests log in and sends to the linked phone number ones the combination of username and mac address have been satisfied and verify the validity of the code when entered.

(v) The system ought to have the capacity to grant access to the authorized resources ones authentication has been achieved.

(vi) In the event that the system has denied access to authorized user, the system ought to allow the system administrator to access the backend and reset the system or do manual authentication.

4.2.2 Non-Functional Requirements

Non-functional requirements include requirements that are used to judge the operation of the system (Rubin & Chishell, 2008). The following are some of the non-functional requirements considered during the development of the proposed solution:

(i) Usability – The system should be simple and easy to learn and use by all users.
(ii) Response time – The waiting time for the entire authentication and validation process to allow or deny access should be within acceptable range.
(iii) Performance and Reliability – The system must be efficient enough while processing authentication requests and be able to provide satisfactory services to the users.
(iv) Availability and Accessibility – For the system to work a proper internet and GSM connection is necessary.
(v) Robustness – The system must be able to handle unexpected error and echo back with proper responses. It should handle error effectively and error message will be displayed if any unexpected error occurs.
(vi) Supportability Requirements – The application should run on a standard laptops and smart devices without a need to change any system configurations.

4.3 System Architecture

Figure 4.1 gives an illustration of the system architecture. The process begins when machine A requests log in. The device user is requested to input a username and password. The username/password are concatenated with the machine MAC address which are used to track the log in process and provide extra layer of security. The username/password together with the machine MAC address are then verified in the User Authentication Repository via the authenticator. Ones these have been verified, the primary phone number associated with those details is returned to the authenticator. The code generator then generates a one-time random passcode with an expiration time stamp and the dynamic library link knocks on the network providers' servers which then sends the code as an SMS notification to associated phone number. When this code is entered in the user interface, it is validated by the authenticator and the device user at this point is granted access into the system. When authentication has been achieved, the

access authorization level is handled by the access rights authorization register which interfaces the organization resources.

On the contrary, if we do not have a success scenario and a user is denied access, the system administrator would be required to intervene. For instance, if it is a case of wrong input then the user will be asked to re-enter the correct username/password and/or a new random code or contact the administrator. If we have a new device user, they will be required to be registered and approved by the system administrator. The system administrator, as a last course of action, can reset the system should it have technical issues affecting the overall performance of the authentication service being provided.

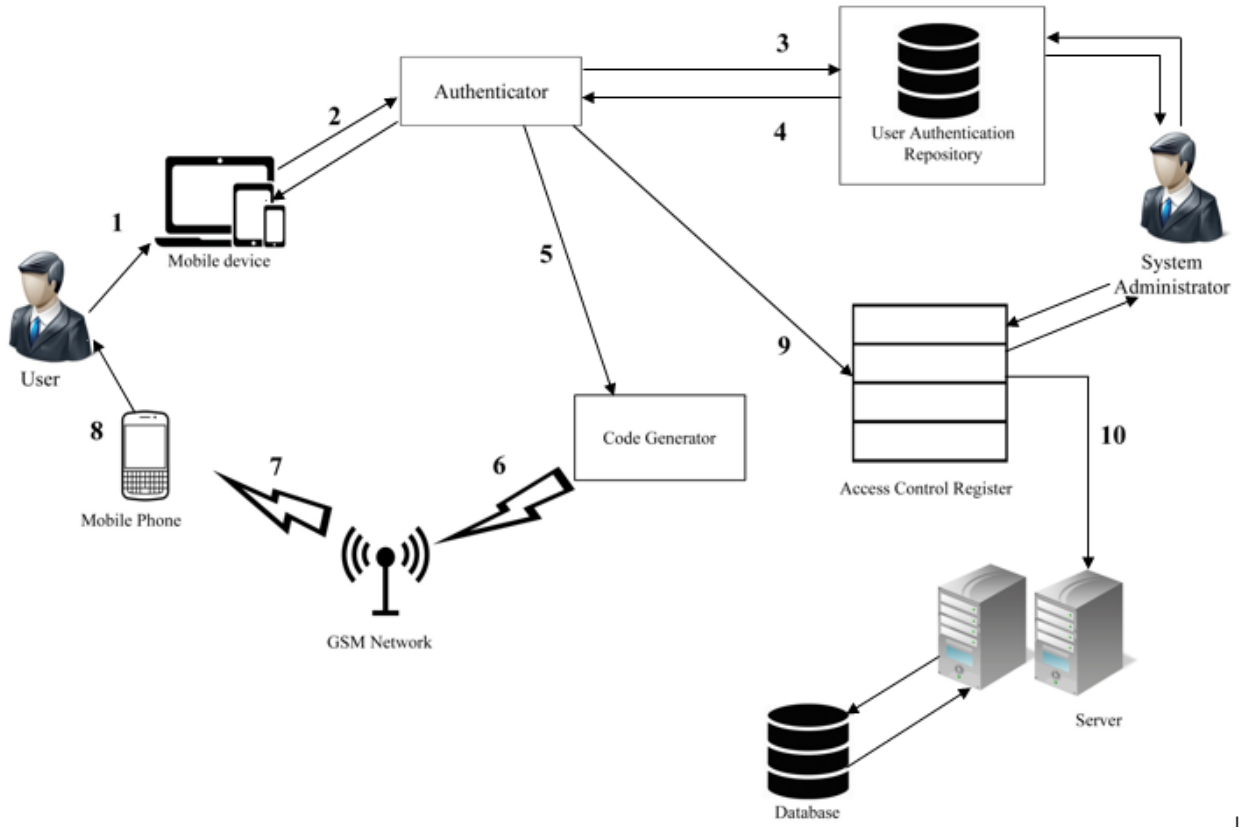


Figure 4.1: Proposed System Architecture

4.4 System Design

Object-oriented design (OOD) techniques was used to refine the object requirements definition identified during system analysis and to define design-specific objects. User requirements were merged with the researcher specifications to come up with the system design with desirable functionalities to meet the objectives. The following design diagrams and corresponding information were used to guide the actual implementation of the system.

4.4.1 Entity Relationship Diagram (ERD)

Entity relationship diagram is a data model used to define and describe process, information or data of a business domain in an abstract way that can be implemented in a database. This consists of entities and the relationships that exists between them (Kruchten, 2012). ERD was used as it clearly shows the system database design, its entities and the relationships between those entities thereby making it easy to be understood. A MySQL database hosted on an Apache server was used to store the data. The logical model of the database is represented in the ERD shown in Figure 4.2.

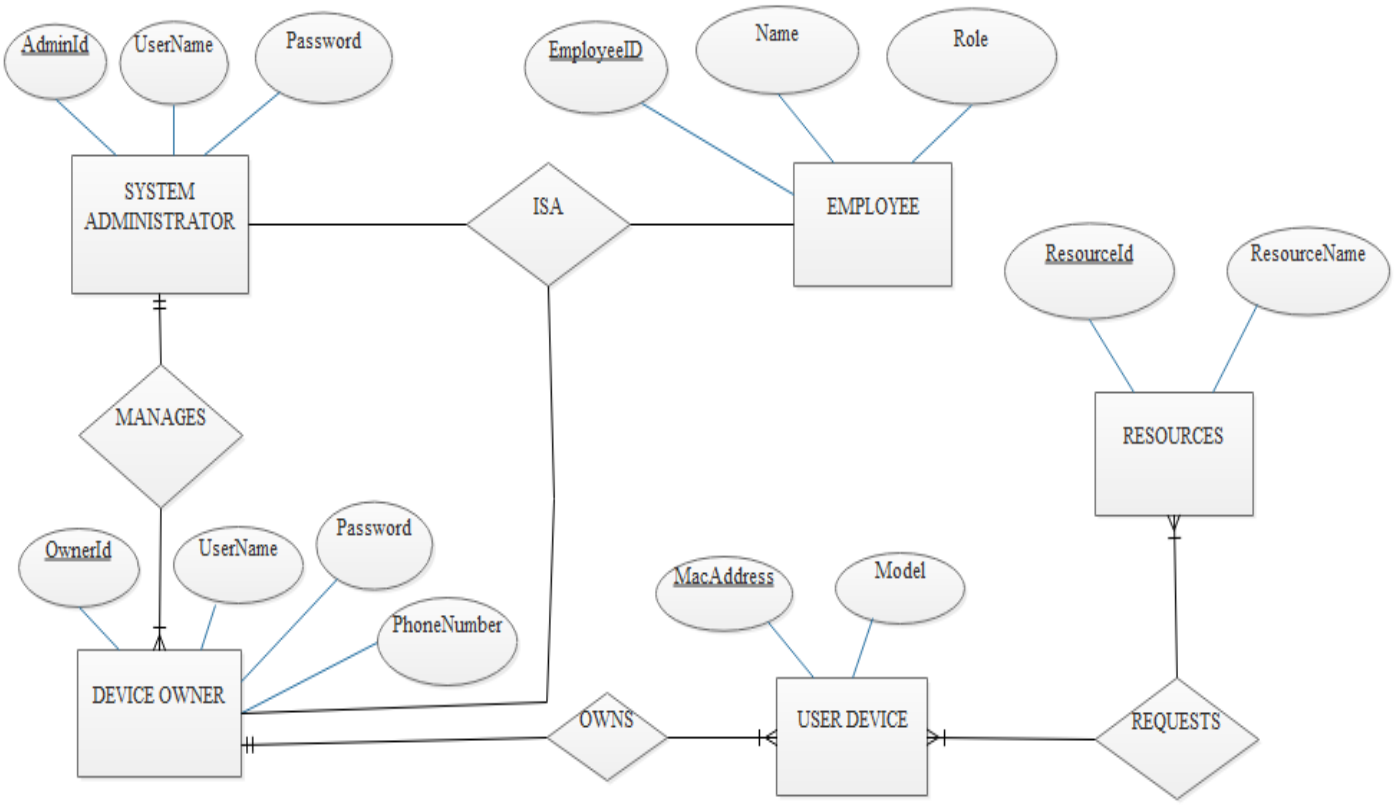


Figure 4.2: A Conceptual Model for the System Database

4.4.2 Class Diagram

According to (Briand & Labiche, 2010), design class diagrams are used to show the existing relationships between classes and visualizations of the system domain model. A class diagram can therefore be said to be a statistic structure diagram that is composed of different system entities, class attributes, methods and the relationships between the classes**.** The relationship between them with the corresponding attributes and operations of implementations are illustrated in Figure 4.3:

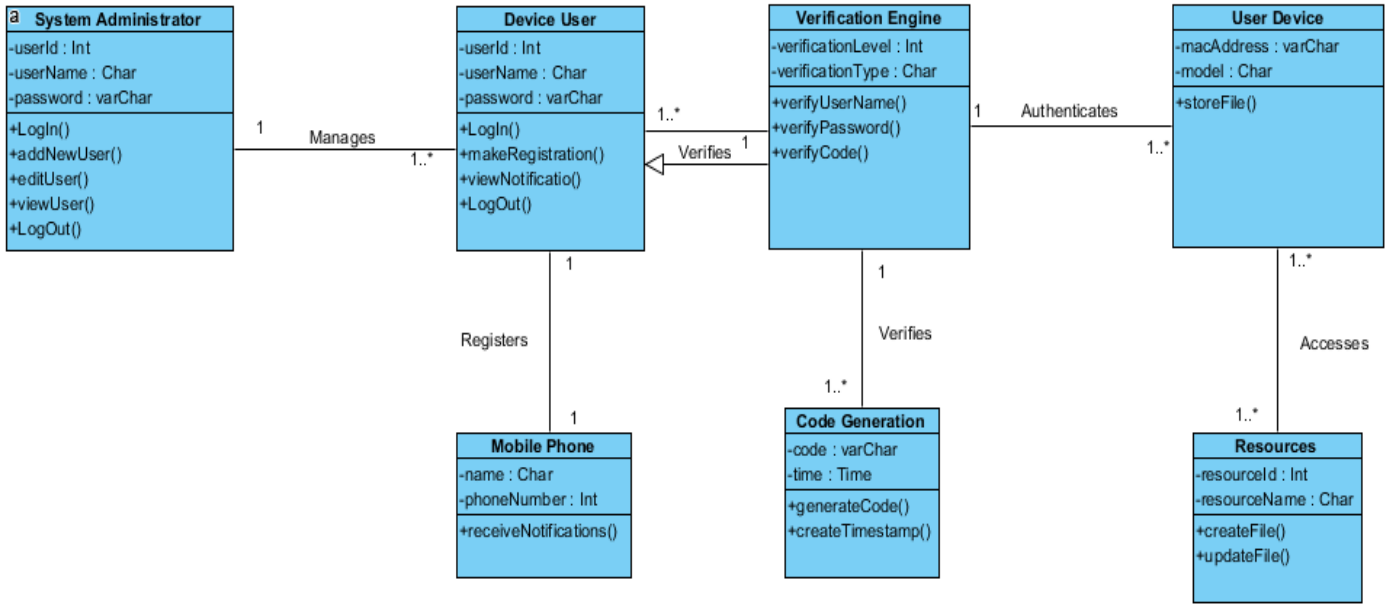


Figure 4.3 Class Diagram of the Proposed system

4.4.3 Process Control

Software process refers to an abstract representation of a software process (Scacchi, 2001)**.** This represents a standardized format for planning, organising and implementing a software project. It comprises of objects, networked sequences of activities and events that entail strategies for handling software evolution.

4.4.3.1 Data Flow Diagrams (DFD)

(i) Context Level Data Flow Diagram

The context diagram in Figure 4.4 depicts the flow of the data to and from the system users to the application. The main users of the proposed system are the device owner and the system

administrator. The device owner provides log in details, that is, username and random code as inputs for identification by the system whereas the system processes those inputs for verification. The system administrator manages the users and the system and can generate logs for audit purposes.

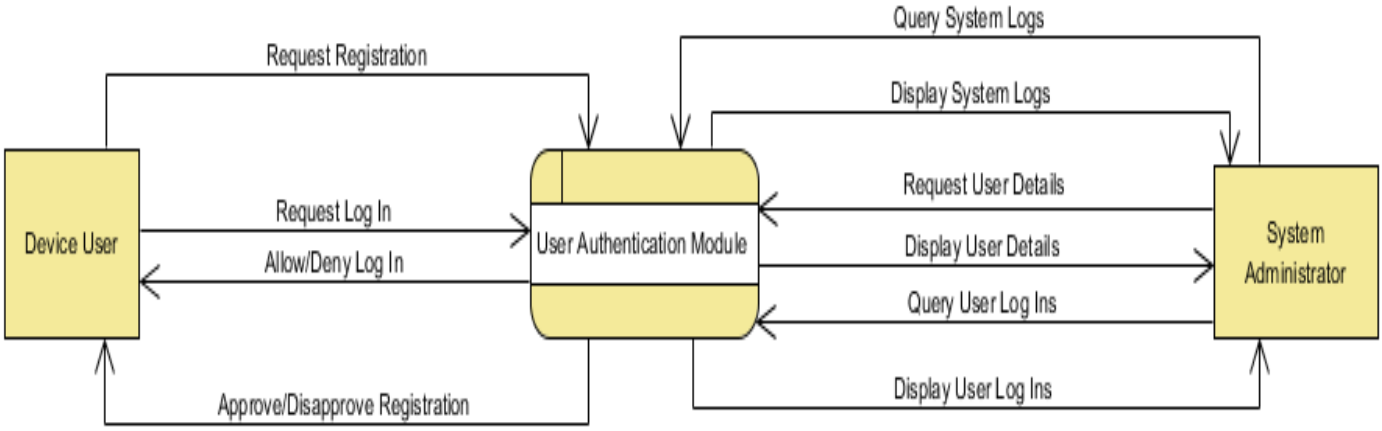


Figure 4.4: The Context Data Flow Diagram

(ii) Level 0 Data Flow Diagram

The Figure 4.5 shows a decomposition of the context diagram to show the various processes in the application and their respective data stores. The two main actors in the system are shown as well as how they interact with the system to achieve their objective. The registration process occurs when a new device owner wants to gain access into the network and use the available resources.

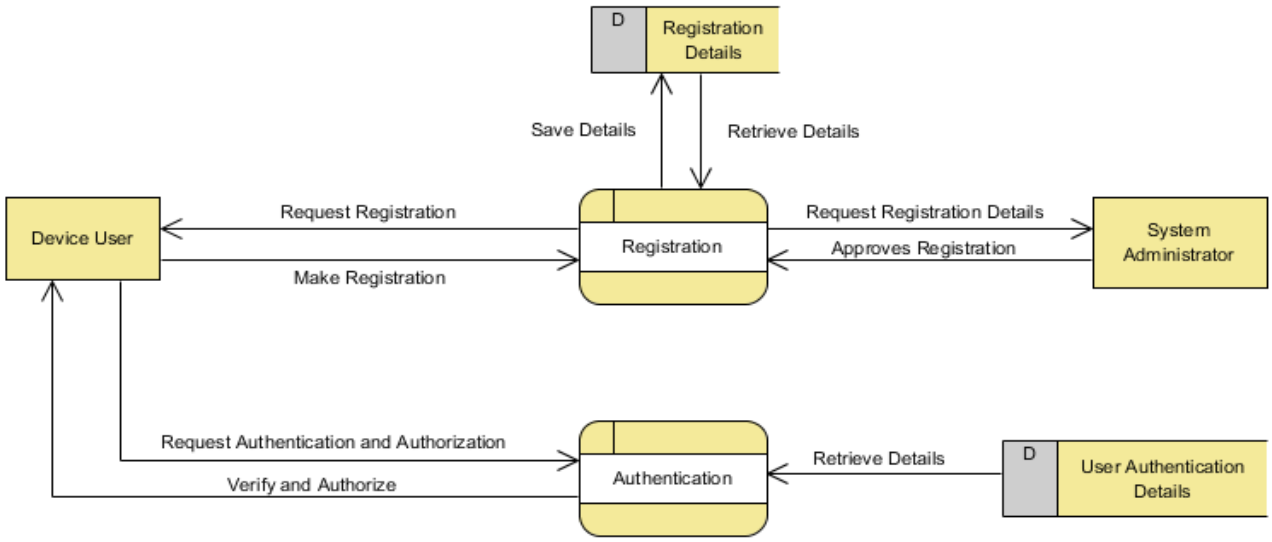


Figure 4.5: The Level 0 Data Flow Diagram

4.4.4 Sequence Diagram

Sequence diagram are used to display the sequential flow of information and interaction between an actor, objects and components within a system as they execute a single use case (Kruchten, 2012)**.** For the designed system, figure 4.6 shows a sequence diagram of an actor requesting login in permission to access the internal servers.

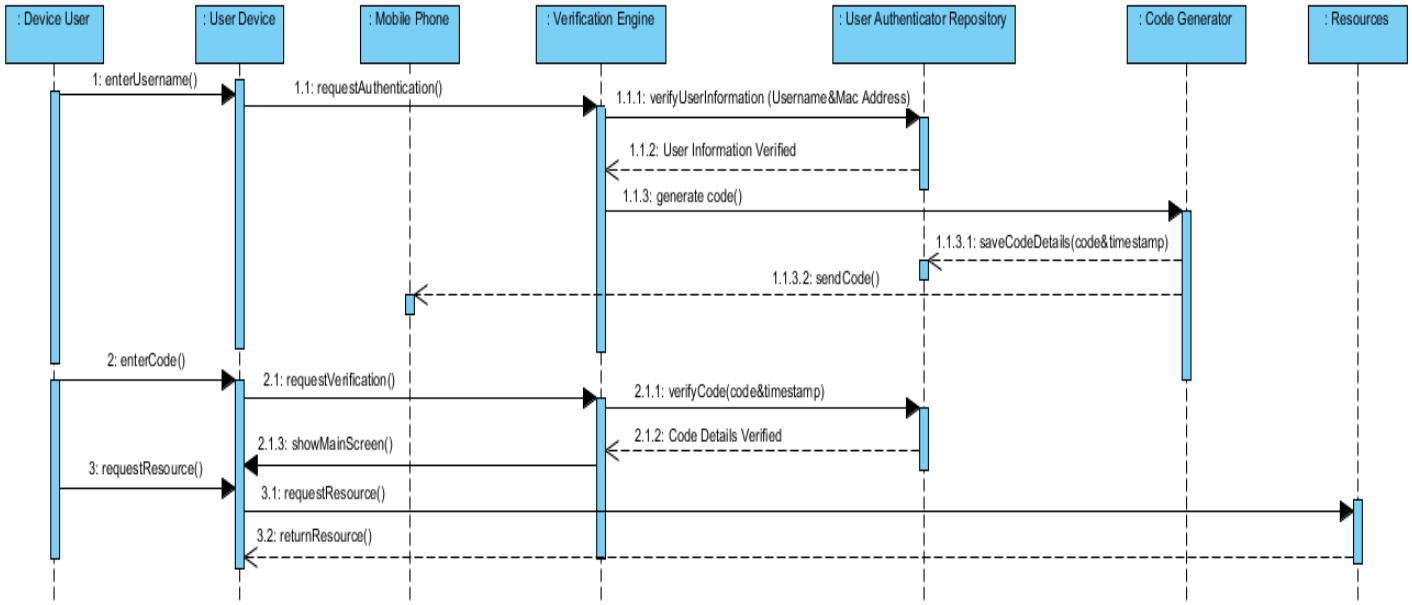


Figure 4.6: Sequence Diagram for Device and User Authentication

4.4.5 Use Case Diagram

The use case diagram on Figure 4.7 depicts the functionality of the proposed system and representation of how the actor and the system interact in a main success scenario. The actors included system administrator, and the device user.

Table 4.1: Use Case Main Success Scenario

Actor Actions	System Response
1. The use case begins when a Device user connects to the internal network either remotely/onsite.	
2. The device user enters their username in the text field on the log in screen.	3. The system authenticator confirms the username entered and returns the primary phone number associated with the MAC address of the device requesting authentication. 4. The code generator sends a one-time random code to the phone number of the device owner. A copy of the code and its time stamp is saved in the authentication repository.
5. The device user enters the random code sent to them into the device user interface to complete the authentication process.	6. The authenticator validates the authenticity of the code as well as the time stamp to ensure it has not expired before allowing user access.

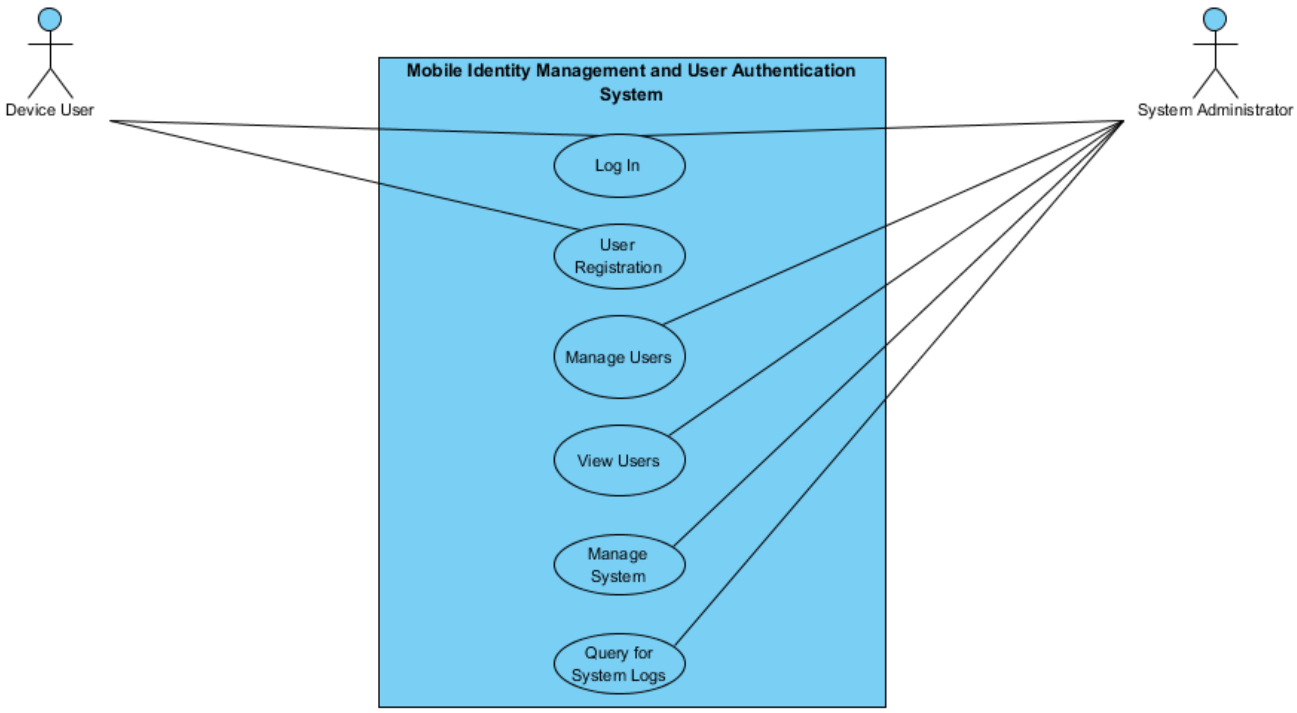


Figure 4.7: Use Case Diagram of the Proposed System

4.5 Security Protocol

It refers to a sequence of operations that ensure protection of data. Used with a communications protocol, it provides secure delivery of data between two parties. When the entities in the device identity and user authentication architecture communicate, there are set of rules and conventions that govern that.

Access control security protocol will be used to provide authentication of user identities as well as authorize access to specific resources based on permissions level and policies. Encryption Algorithm security protocol on the other hand, will be used to store user details such as the passwords.

4.6 System Wireframe

Figure 4.8 is an illustration of the system's wireframe which shows how the elements within the system will flow in the user interface as the various users interacts with it.

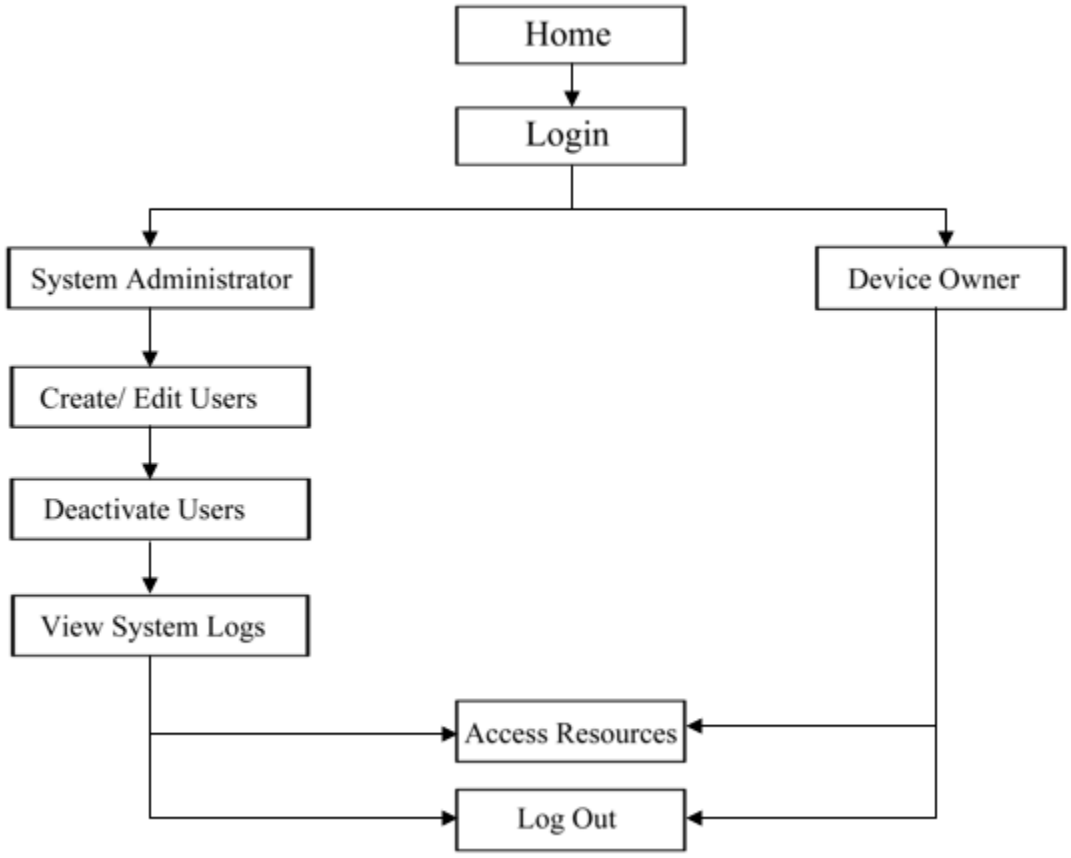


Figure 4.8: System wireframe

Chapter 5: Prototype Implementation and Validation

5.1 Introduction

The chapter covers both implementation and validation of the proposed system. The implementation part, focuses on the different parts of the system, looking at the implementation methodology followed and how those parts function. The testing part of the chapter focuses on usability testing and functional testing to verify if the application attains the objectives of the proposed solution.

5.2 Prototype Implementation

The application comprises of front-end and back-end subsystems: the front end is a desktop application system while the back end is a dynamic library system and the dot(.)net framework which was used as the programming language to develop the authentication application.

5.2.1 Application Hardware Requirements

The Table 5.1 shows the minimum hardware requirements for successful implementation of the proposed system.

Table 5.1: Hardware Requirements

Hardware	**Description**
Processor	Core2Duo and above
Memory	2GB
Hard Disk Space	250GB
Network Connectivity	Internet access

5.2.2 Application Software Requirements

The Table 5.2 shows the minimum software requirements for successful implementation of the proposed system.

Table 5.2: Software Requirements

Software	Description
Operating System	Microsoft Windows OS
Relational Database Management System	MySQL 5.0.45
Programming languages	Dot(.)Net framework
Internet Browser	Google Chrome, Mozilla
Application used	Microsoft Excel
IDE	Visual Studio 2010

5.2.3 Prototype Development

The two subsystems are explained below:

5.2.3.1 Application Front-End

The front end of the system is a desktop application that system users install in their devices. This is the platform through which they will use to interact with the main user authentication database for device identity and user authentication. This front end used vb.net for programming. The following are the main screen shots. See Appendix D for further images.

Figure 5.1 is the main window through which the system user is prompted to create a new user account on first log in after installation of the system setup.

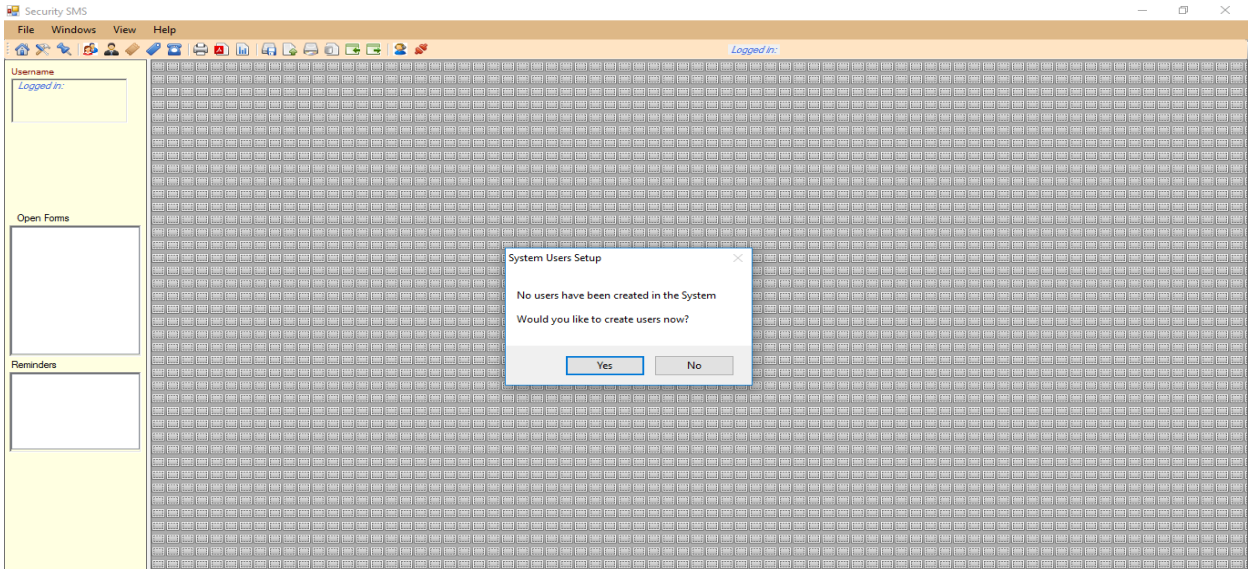


Figure 5.1: User Log in Screen

Figure 5.2 shows the user details window, through which the user enters their details for registration and subsequently stored in the User Authentication Repository (UAR).

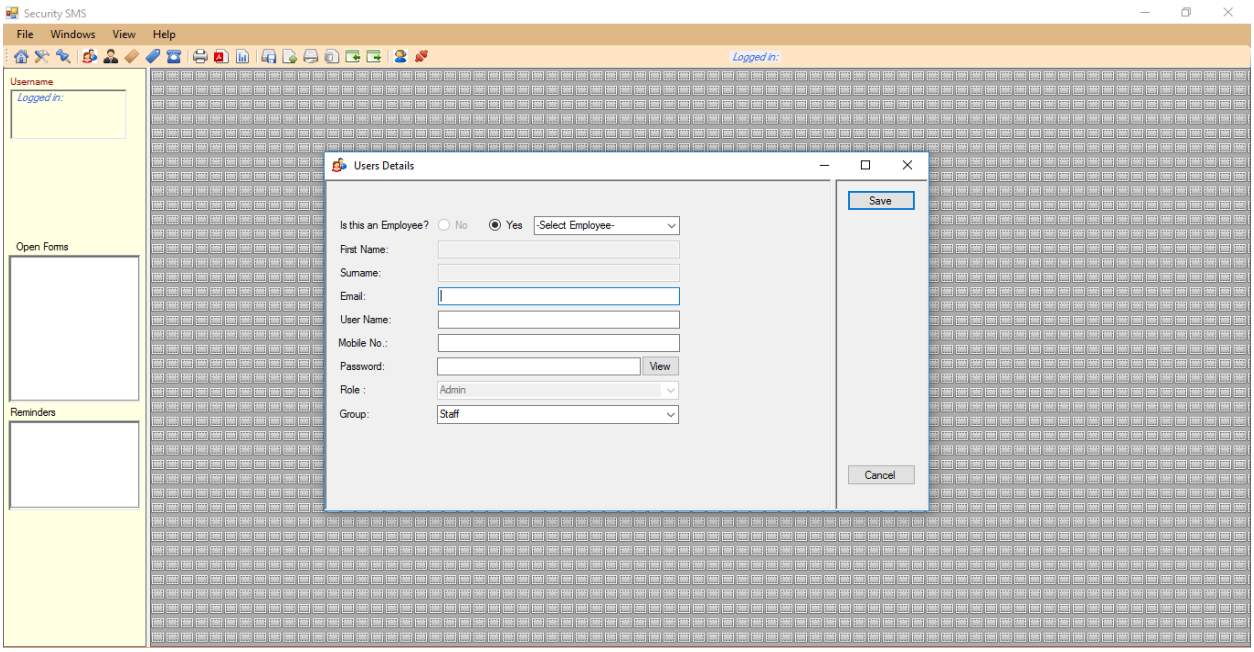


Figure 5.2: User Details Screen

Figure 5.3 is the passcode verification window which is displayed after the user details have been authenticated by the system which then sends the random code to user mobile device. This is the code which is subsequently entered into this window for validation.

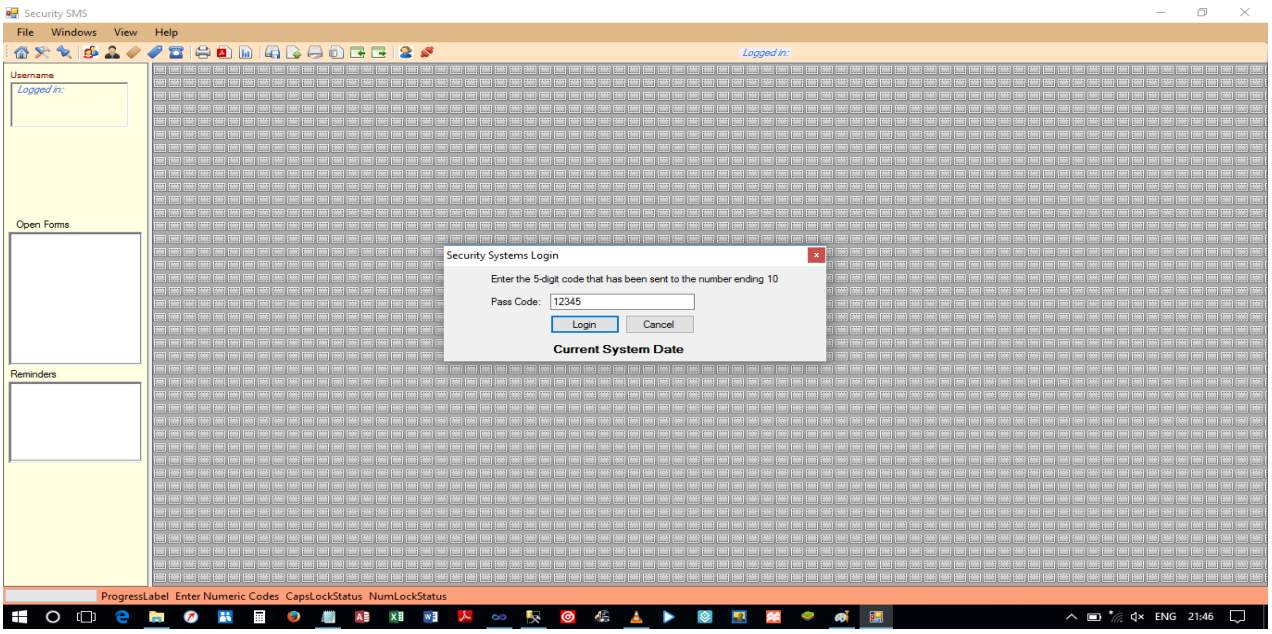


Figure 5.3: Random Code Validation Screen

5.2.3.2 Application Back-end

The application back end has a system administrator dashboard for the management of users and the system as well. Some of the functionalities performed at the backend include admin login and logout, admin adding, editing and deleting users, admin viewing system logs, admin viewing all the menus, and interacting with the database directly. The backend was developed using vb.net and MSSQL server for database management system. See Appendix D.

5.2.4 System Users

The system was designed with two primary users in mind, namely system administrator and device owner. Both of whom interact with the system through respective interfaces as they seek to extract some functional benefits.

5.2.4.1 System Administrator

The System Administrator (SA) is responsible for smooth running of the system through effective provisioning, installation/configuration, operation, and maintenance of **systems** hardware and software and related infrastructure. Some of the key roles played by the SA involve adding and removing users and devices, editing user details, maintaining the system and supporting system users among others.

5.2.4.2 Device Owner

The device owner is primarily responsible for providing their registration details if they are new users. Whereas for existing device owners they are responsible for ensuring the physical security of their devices.

5.3 Prototype Validation

Agile testing was used in the research which involves testing software for bugs or performance issues within the context of an agile workflow. Testing is usually a quality gate and the QA test group often serves as the quality gate keeper. Testing prevents bad software going out to the field. Agile testing enables building the product well from the beginning using testing to provide feedback on an ongoing basis about how well the emerging product is meeting the business needs (Hendrickson, 2008). Agile testing was applied continuously during the software development to ensure that the features implemented during a given iteration are actually done.

Table 5.3: Prototype Validation Results

Step	Action	Expected Response	Comments
1.0	**User Registration**		
1.1	The user selects Add New option	A new window with input fields for creating a new member is presented to the user	Pass
1.2	User makes Invalid Data entry	Error Dialog box	Pass
1.3	User leaves out a Mandatory Field	Error Dialog box	Pass
1.4	User submits details	The registration status is turned to "Pending"	Pass
2.0	**User Login/Authentication**		
2.1	Registered user enters Correct Username and Password	Application display Passcode Text Field for user to input the random code	Pass
2.2	User receives random passcode from telecom service provider	Application display the passcode text field	Pass
2.3	User enters wrong Username, Password or Code	Error Dialog box displayed	Pass
3.0	Registration Approval		
3.1	System Administrator approves device user's registration.	Device owner status changes to "Approved" or "Denied".	Pass
		If approval is successful User Authentication Repository is updated.	Pass

5.4 Usability validation

The core of this proposed system is in its ability to bring together People, Process and Technology in a way that would increase the chances of having a successful BYOD adoption in the organizations. There exist various challenges in the adoption of BYOD into the organization and these vary with regards to the various verticals and industries. However, the key measure of a model/system is in its ability to provide a solution or solutions that are quantifiable. The

usability validation used five key measurement metrics that organizations can use to ascertain how well the proposed system if adopted would ensure maximum value.

The measurement of the various metrics varies and the respondents used in the study were from various organizations within the financial industry, however we narrowed down only to a select few in order to validate the system.

5.4.1 User Friendly

On User Friendly attribute, the respondents were asked to rate whether the prototype was "Simple", "Moderate" or "Somewhat Friendly" to use and operate. The responses from the selected 30 respondents were represented as shown in Figure 5.4.

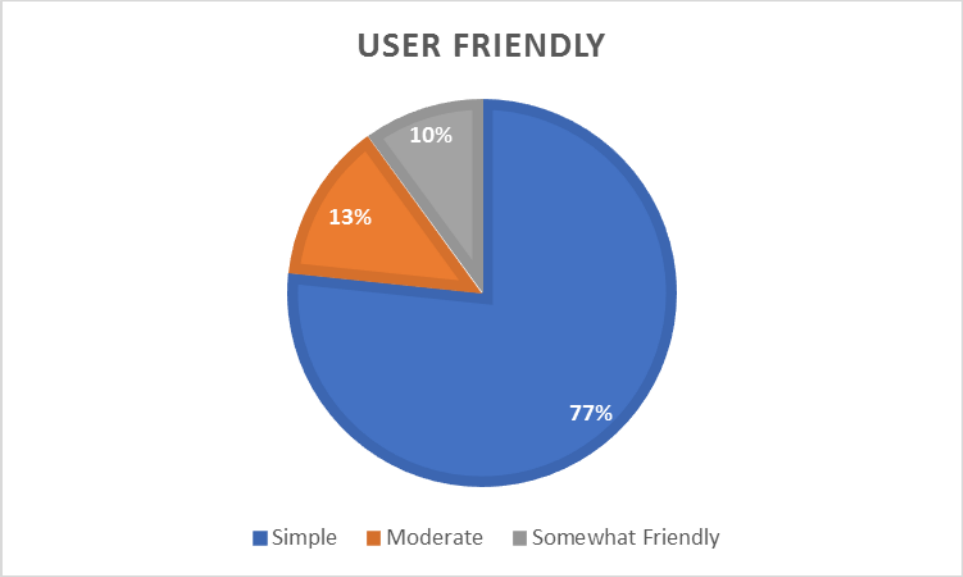


Figure 5.4: User Friendliness Validation

5.4.2 Responsiveness

On Prototype Responsiveness, the validation sort to obtain feedback as to the degree of promptness (delay time) when a user requests to be registered and/or authenticated by the system. The respondents were asked to select either "Excellent", "Very Good", "Good" or "Fair". This data is captured in Figure 5.5.

Figure 5.5: Prototype Responsiveness Validation

5.4.3 Useful and Satisfying

With regards to meeting the main objective of the research in terms of proposing a new approach to improve the security in a BYOD environment, respondents were asked whether they believe the proposed prototype would help solve the problem of identity theft in a mobile environment and whether it would satisfy that need. The question put forward had the following choices: Strongly Agree, Agree, Neutral, Disagree. Figure 5.6 summarises their responses.

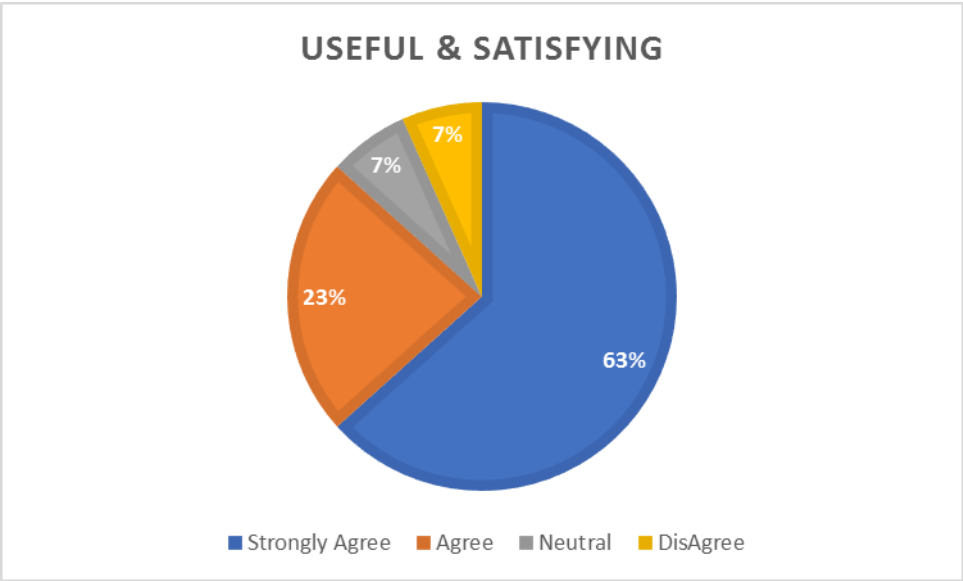


Figure 5.6: Usefulness and Satisfactory Validation

5.4.4 Ability to achieve core Functionality

In terms of the how the system was able to meet its functional requirements and in turn meet user requirements, the research did a validation testing on the core functionalities. The question asked was to what extent do the system users believe the system is able to achieve its core functionality. The choices available were; Excellent, Very Good, Good and Fair. Of the 30 respondents, the results were as follows; 21 Excellent, 5 Very Good, 2 Good, 2 Fair. Figure 5.7 summarises these results:

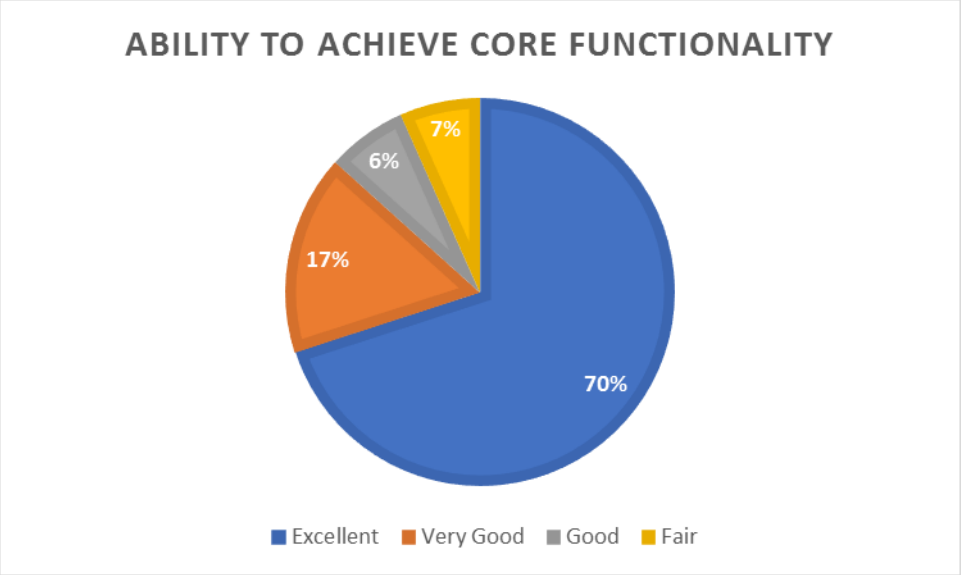


Figure 5.7: Functionality Validation

5.4.5 Acceptability

Acceptability test was carried out to determine how users would accept and adopt the developed solution to address the challenges of identity theft especially in cases where the device and application used are legitimate. Out of the 30 selected participants, 23 accepted the solution, 4 were not sure and 3 Accepted with reservations (only if certain conditions are met). Figure 5.8 shows a representation of this data.

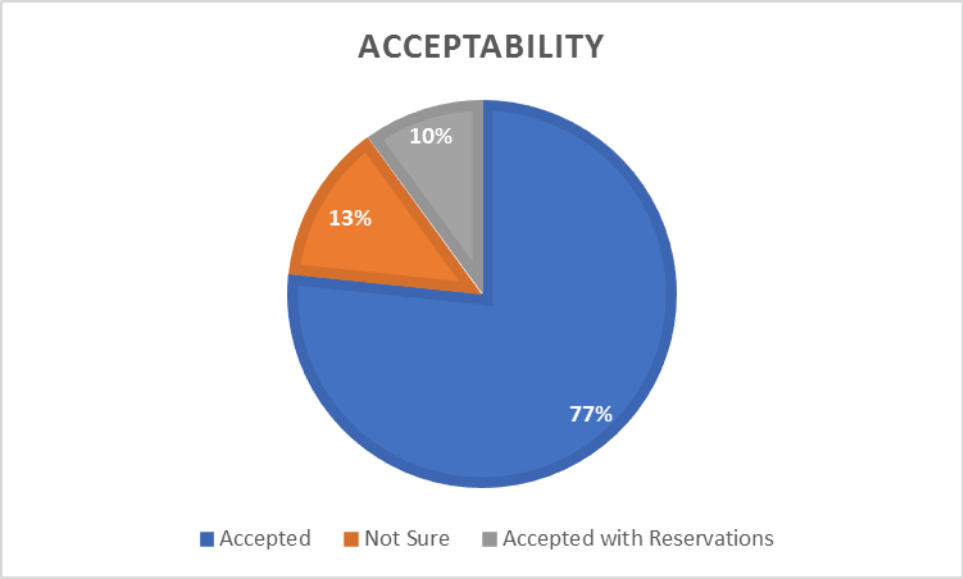


Figure 5.8: Acceptability Validation

Chapter 6: Discussion of Key Findings

6.1 Introduction

This chapter covers discussions of various tests conducted to determine the prototype performance, its relevance and feasibility in a real-world scenario. The discussions show how the results obtained help meet the study objectives. The research test results were obtained from conducting two distinct but interrelated validation procedures, that is, prototype validation and usability validation. Prototype validation was aimed at confirming the quality of the developed prototype while usability validation was performed to evaluate the application by testing it on users to determine the effectiveness of the application in performing some tasks.

6.2 Discussion Summary of Research Findings

The research findings were drawn from the main objectives that were set out for the purpose of this research. Below is a discussion of how each objective was met

6.2.1 Review of existing BYOD models and solutions being used in mobile environments

The research was able to meet this first objective by reviewing the following main models namely Akenti Authorization Model (Abdelilah et al., 2003), Privilege and Role Management Infrastructure Standards Validation (PERMIS) (Chadwick et al., 2008), Community Authorization Service (CAS) (Pearlman et al., 2002), Data-centric Information Security Model for Bring Your-Own-Device Environment (Juma, 2014), Adoption model to guide Bring Your Own Device concept (Mwenemeru, 2013) and lastly a model to enhance information security in the use of the BYOD (Ndwiga, 2015). Looking at the models together with the three main BYOD solutions which were reviewed namely mobile device management, mobile application management and mobile content/information management, it was concluded that the models present for authentication, even though they were able to provide authentication services within mobile communities the downside is they were highly complex in nature and costly and thus could not be implemented in their current state. In the case of the models being proposed by Mwenemeru, 2013, Juma, 2014 and Ndwiga, 2015 and the three BYOD solutions, they were mainly focused in handling data security, devices security and applications security but do not

provide authentication services. This is the gap which this research set out to fill to further add the existing security models and solutions to achieve identity management and user authentication in the successful adoption and implementation of BYOD in our organizations.

6.2.2 Factors that influence the mobile identity management and user authentication for BYOD devices.

The second objective was to identify the main factors that influence the mobile identity management and user authentication for BYOD devices and as such justify the need for the solution. From the review of various literature sources in relation to BYOD and mobile device identity management and user authentication challenge, the research noted that with the BYOD security perimeter mainly encompassing the user, device and data, serious security concerns rise in terms of Confidentiality, Integrity, Availability, Authentication and Access control and Authorization. With the current solutions being capable to carter for confidentiality, integrity and availability, they lacked in offering proper authentication mechanisms and unique device identification mechanisms. The research managed to assess these two factors in depth and introduced a solution that is capable of filling this security challenge. The test results can further support the ability of the system to meet its functional requirement and the overall acceptability of the system.

6.2.3 Planning and adoption of integrated identity management and user authentication solution for organizations.

The third objective was to plan and develop a device identity and user authentication management application for the verification of devices and users within organizations. This would provide the first security check entry point before employees are authorized to use corporate applications and gain access to internal resources. During the planning phase, the activities that were to be carried out and how were carefully selected and arranged. The agile SDLC model provided a framework that was used for development of the solution. Because the research was undertaken to design a working prototype as proof of concept, an adoption strategy that involved system building, implementation and testing was drawn in details. These have been discussed in details in chapter 5 and 6.

6.2.4 Prototype validation Test Results

The fourth and final objective of the research was to validate the proposed solution. Prototype validation tests were about functional and non-functional requirements of the system.

6.2.4.1 Functionality Test Results

It is clear that all functional requirements were successfully validated. Table 5.3 shows the results. Which means that the system could be implemented in a real environment and achieve the main objective of this research.

The following conclusions can be drawn from the presented results obtained from the functionality tests results:

(i) The system was able to correctly and accurately capture the primary details of a device user. The same details were stored in the User Authentication Repository. However, wrong inputs of these details such as inputting numeric character in place of alphabets or leaving blank spaces in mandatory fields would lead to incomplete registration.

(ii) The system was also able to effectively verify the username, password and mac address details and send a verification passcode to the particular device owner. This passcode was also verified correctly to ensure it has been sent by the authentication system and has been entered within the allowed time span.

(iii)The system was able display an error message if the username, password and/or random code is wrong and/or has an expired.

6.2.4.2 Usability Test Results

Usability validation was based on 5 key validation criteria to test the effective functioning of the prototype when deployed for user interaction. On the user friendliness of the system, a majority representing 77% said it was simple to use compared to the 13% and 10% who said it was either moderate or somewhat friendly respectively. This showed that users were able to quickly learn how to use the system and achieve their goal.

When the system responsiveness was tested, 17% said it was excellent while 60% said it was very good. When put into perspective this meant that 77% of users found that the system was able to process their log in requests at a highly acceptable speed with little waiting time. This

was important because unacceptable response time (delay time) would cause anxiety and impatience among many users.

When the usefulness and level of satisfaction of the system was tested, 63% of the respondents strongly agreed that it was both useful to them and satisfied their identity management and user authentication need. The other 23% agreed while 7% were either neutral or disagreed. This showed the level of importance of the proposed solution in our Kenyan organizations and especially among those who were selected for the purpose of this research.

Last but not least, Functionality validation had 70% respondents saying the system met its functional requirements excellently. The other 17% and 6% either said it did meet its functionality very good or good. The remaining 7% gave a fair assessment of the systems capability to meet its functional requirements. Since this was an iterative process, there were cases where the system would fail and those failures contributed to majority of the 7% who gave the "fair" response. These system failures were resolved in the subsequent iterations.

Finally, acceptability test was done to rate whether the system would be adopted by the various organizations. 77% of the respondents indicated they would accept to the adopt the solution in case it was made commercial while 13% said they were not sure and 10% accepted the solution with reservations. Of the 13% and 10% of those who said they were not sure or accepted with reservations the main concern was in terms of the overall investment cost they would have to incur and whether the returns on investment would be worth it. The costing of the solution was not done as at this stage of the research.

The table 6.1 shows a summary of the results discussed. Note that the table only shows the percentage of the positive results that seek to support the validity of the proposed solution.

Table 6.1: A summary of Validation test results.

METRIC	**RESPONDENTS**
User friendliness	77%
Responsiveness	77%
Usefulness and level of satisfaction	63%
Functionality	70%
Acceptability	77%

In summary, the test results were discussed elaborately for clarity and to give merit for the need of this research work. The prototype tests were based on functional and non-functional requirements of the system. The functional tests were on the prototype itself while non-functional were for the usability tests. The testing of the implemented solution took place among the participants that were obtained during the planning phase. After initial education, distribution, and installation, testers were informed to focus on issues of functionality, user interface, learnability, and usability. Sampling of the eventual testing results indicated a positive response to the implementation, displaying a good acceptability margin, and potential of quick adoption among users.

Chapter 7: Conclusion and Recommendations

7.1 Overview

This chapter presents conclusions and recommendations based on the in-depth analysis of the proposed identity and access management model to guide in the adoption and implementation of BYOD concept within organizations in Kenya.

7.2 Conclusions

The process of ensuring internal (and external) network security is a repetitive and integrated one. Security administrators will in this manner keep on looking for new ways and approaches to make the procedure proficient and savvy. Different strategies are at present being utilized to ensure corporate resources are secured and it is vital to show some of these strategies keeping in mind the end goal is to contrast them and come up with a better approach as proposed in this research work.

From the review of various publications and analysis of different solutions, the study determined that number of factors inform the decision by organizations to adopt BYOD phenomenon top among them being efforts of organizations to reducing complexity and cost of managing mobility and employees wanting to use the most popular devices that they use as consumers, instead of the devices provided by the employer (Garlati, 2011).When we consider the benefits, Bring Your Own Device provides organizations with benefits in 3 broad areas i.e. **Strategic Benefits, Productivity Benefits (**Enhanced performance, flexibility, job collaboration, job satisfaction**)** and **Cost Saving Benefits** (Acquisition of personally owned devices to achieve corporate tasks).

The research study was conducted with the main objective being to develop a solution to mitigate on the identity theft and user authentication challenge in a mobile environment. A breach in the corporate network by unidentified person(s) can lead to the exposure of resources such as servers and databases thus putting the organization at risk. The impact of this vulnerability more so, in financial institutions in the case of this research, if a successful attack happens can be immense and therefore, the need to put proactive measures in place to prevent such attacks. Kenyan institutions, which is a fast-developing country, are gradually accepting and embracing BYOD with mixed attitudes towards implementing it. Through the review and

observation of the various implementation strategies, it was clear that when BYOD is implemented well, the benefits of it are immense and thus having a secure implementation approach is imperative to enjoy the benefits. It is with this in mind that the proposed study aimed to develop and implement solution to ensure improved security in the use of BYOD within Kenyan institutions.

In the quest to develop the proposed identity management and user authentication solution, the research study first set out to collect relevant data that would inform the problem/gap to be addressed. These data were collected from both primary and secondary sources. A mixed method of research type was used in the research methodology. To gain first-hand information, the researcher visited the financial institutions within Nairobi, Kenya and identified persons of interest. These people formed the focus groups that gave a deeper understanding on the implementation of BYOD. From the interactions/interviews with these individuals, it was confirmed that mobile identity and access management solutions ranked the least in terms of implementation among the other three solutions namely mobile device management, mobile information management and mobile application management. The weaknesses that arise as a result of this further confirmed the findings made from the literature reviewed which paint a picture of unauthenticated access for users who gain access via authorized applications running on devices which may be lost, stolen or left without signing out.

The study therefore sought to integrate an authentication module with the existing system as a potential solution in order to obtain maximum benefits from the implementation of BYOD. The proposed solution developed would be run on a client-server type of architecture. This is because the device owner would have a user interface on their device to make log in request whereas the authentication system would sit within the internal network of the organization to serve that request. This would ensure efficient management and security of the system.

7.3 Limitations of the study

Time: The study involved two very distinct and important surveys to be able to come up with an accurate solution. The first of which was a pre-study to have factual basis on the current BYOD solution within the Kenyan organizations and secondly, a post implementation survey to collect data on user experience and viability of the proposed system. This would require certain

bureaucratic red-tape challenges to be overcome to implement the system especially within a financial institution.

Respondents readiness: For the complete development, implementation and testing of the proposed system a considerably long period of time would be required. With different institutions (respondents) having different budgets and complexities of their enterprise infrastructure, this would result to the achievement of readiness level at different paces.

7.4 Research Contributions

The main contribution of this research is to solve an issue that affects many organizations, which, if actualized, can enhance the benefits of BYOD. By using authentication mechanisms such as those used by Yahoo, Google and LinkedIn and designing a prototype that can be incorporated with the existing BYOD solutions and applying that technology in our local scenario, the study has shown how common problems can be solved by use of existing technologies in new areas. The fact that this study has been able to develop a prototype model for demonstration purposes is also a noteworthy contribution to what must be viewed as the practicality of the idea if fully adopted and implemented by organizations.

7.5 Recommendations/Suggestion for Future Research

One qualitative study cannot explain every possible scenario of what can happen when mobile devices such as laptops, tablets and smartphones are used as working tools especially when different organizations have different needs and produce different kinds of data. Most importantly, the mobility of employees and their behavior varies. This research recommends the following areas for further study:

(i) *In depth analysis of how Mobility, Device User Behaviour and Policy formulation are impacting the future of Bring Your Own Device adoption*

The research findings showed that most organizations are looking for better ways to adopt BYOD while taking into consideration that People, Processes and Technology are key pillars in

the successful adoption of BYOD. As mobility becomes integral part of modern day organizations, it is thus becoming imperative that a comprehensive model or framework be in place to guide in incorporating such devices in the broader business operations with an eye on the human behavior such as multi user/sharing of devices.

(ii) *The impact of remote access on the Bring Your Own Device adoption strategies to organizations.*

The capabilities of remote access to internal corporate resources by both employees and external partners in the BYOD environment ought to be further probed. For instance, modern day agency banking in the financial sector needs to be well regulated in order to be able to provide a clear way of addressing key issues that may arise in case of device loss, information/application compromise and identity theft.

(iii) *Employee self-service*

Since it's typically either impractical or impossible for organizations to take possession of employee-owned devices, it is essential that employees are able to provision and service devices through a "single self-service window." Device and data-plan management, usage tracking, and access to authorized corporate applications should be included.

(iv) Auto-certification and Teleworking

With employees connecting to the network and provisioning their own devices, the enterprise must establish the process for automatically certifying that the device has a container and is consistently connecting through that container. An organization's virtual desktop and unified communication strategy should extend to mobile devices. This is an area of further research.

References

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

Alberta Education. (2012). Bring Your Own Device: A Guide for Schools. Retrieved from http://www.education.alberta.ca/media/6724519/byod%20guide%20final.pdf

Allam, S. (2011). An Adaptation of the Awareness Boundary Model towards Smartphones Security.

Best, J. ., & Kahn, J. . (1998). *Research in Education* (8th ed.). Needham Heights, MA: Allyn & Bacon.

Botha, R. ., Furnell, S. ., & Clarke, N. . (2009). From Desktop to Mobile: Examining the Security Experience, *28*(3–4), 130–137.

Brandly, T. (2011). Pros and Cons of Bringing Your Own Device to Work. Retrieved from http://www.pcworld.com/businesscenter/article/246760/pros_and_cons_of_bringing_your_own_device_to_work.html

Bredemeyer, C. (2001). *Defining Non-Functional Requirements: Architecture Resources for Enterprise Advantage.*

Briand, L., & Labiche, Y. (2010). *A UML-based approach to system testing* (1st ed., Vol. 1).

Burt, J. (2011). BYOD trend pressures corporate networks. *eWeek*, *28*(14), 30–31.

Chadwick, D., Zhao, G., Otenko, S., Laborde, R., Su, L., & Nguyen, T. (2008). PERMIS: A Modular Authorization infrastructure. Concurrency Computation Practice Expert, (20), 1341–1357. https://doi.org/10.1002/cpe.1313

Cockburn, A. (2002). Agile Software Development (p. 278). Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Cresswell, J. . (2003). Research design: Qualitative, Quantitative and Mixed Methods approaches. Sage.

Crisp, C., & Williams, M. (2009). Mobile device selection in Higher Education: iPhone versus iPod touch. Retrieved from http://www.acu.edu/technology/mobilelearning/documents/research/crisp/mobiledeviceselection.pdf

Crook, S. . (2011). Embracing Consumerization with Confidence. Retrieved from www.trendmicro.co.uk/media/wp/embracing-consumerization-with-confidence-idc-analyst-whitepaper-en.pdf

Ernst & Young. (2013). Security and Risk considerations for your mobile device program.

Eslahi, M., & Var, N. M. (2014). *BYOD: The Current State and Security Challenges.* Presented at the Computer Applications & Industrial Electronics, IEEE Symposium.

Forrester. (2012). Latest IT Trends For Secure Mobile Collaboration. Retrieved from http://www.connectedfuturesmag.com/docs/byod_forrester_tap_latest_it_trends_wp_en.pdf

Garlati, C. (2011). Trend micro consumerization report 2011. Retrieved from http://bringyourownit.com/2011/09/26/trend-micro-consumerization-repor

Gartner. (2011). Bring Your Own Device: New Opportunities, New Challenges. Retrieved from https://www.gartner.com/doc/2125515/bring-device-newopportunities-new

Green, A. (2007). Management of security policies for mobile devices. In *Information Security curriculum development*. Kennesaw, GA, USA: Association for Computing Machinery.

Hendrickson, E. (2008). Agile Testing.

ISACA. (2012). ISACA Survey: Latin American companies increasingly worried about BYOD risk. ISACA. Retrieved from http://www.isaca.org/About-ISACA/Press-room/NewsReleases/2012/Pages/ISACA-Survey-Latin-America-Companies-Increasingly-Worried-About-BYOD-Risk.aspx

Juma, I. (2014, June). *Data-centric Information Security Model for Bring Your-Own-Device Environment*. Strathmore University, Nairobi, Kenya.

Kothari, C. . (2004). *Research Methodology: Methods & Techniques.* Retrieved from http://books.google.co.ke/books

Krishnan, H. (2011). Consumerization: Managing the BYOD trend successfully. Wipro Inc.

Kruchten, P. (2012). The View Model of architecture. IEEE Software, *12*(6), 42–50.

McAfee. (2011). McAfee tech report. Retrieved from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-20 11.pdf

Miller, K. W., Voas, J., & Hurlburt, G. . (2012). BYOD: Security and Privacy Considerations. *IT Professional*, *14*(5), 53–55. https://doi.org/10.1109/mitp.2012.93.

Morrow, K. (2012). Network Security, *4*(12), 5–8.

Mwenemeru, H., K. (2013, June). *A Model to Guide in the Adoption of Bring Your Own Device concept in an Organization*. Strathmore University, Nairobi, Kenya.

Ndwiga, A. (2015). *A Model to enhance Information Security in the use of the BYOD in Kenyan enterprises*. Strathmore University, Nairobi, Kenya.

Owens, L. . (2002). Introduction to Survey Research Design. Retrieved from http://www.srl.uic.edu/seminars/Intro/introsrm.pdf

Pearlman, L., Welch, V., Foster, I., Kesselman, C., & Tuecke, S. (2002). A Community Authorization Service, 50–59. https://doi.org/10.1109/Policy.2002.1011293

Rubin, J., & Chishell, D. (2008). *Handbook of Usability Testing* (2nd ed.). Wiley Inc.

Scacchi, W. (2001). Process Models in Software Engineering. *University of California Institute for Software Research. New York: John Wiley and Sons Inc.*

Scarfo, A. (2012). New Security Perspectives around BYOD. Presented at the Seventh International Conference on Broadband, Wireless Computing, Communication and Applications. https://doi.org/10.1109/bwcca.2012.79

Sen, P. . (2012). *Consumerization of Information Technology drivers, benefits and challenges for New Zealand corporates.* Retrieved from http://researcharchive.vuw.ac.nz/bitstream/handle/10063/2095/thesis.pdf?sequence=1

Trend Micro Incorporated. (2012). BYOD and consumerization of IT. Retrieved from http://www.trend micro.com

Appendices

Appendix A: Questionnaire

Dear respondent,

My name is …….. I am a post graduate student at Strathmore University conducting a research on "**IDENTITY MANAGEMENT AND USER AUTHENTICATION APPROACH FOR THE ADOPTION AND IMPLEMENTATION OF BRING YOUR OWN DEVICE IN ORGANIZATIONS**" as a partial fulfillment of the requirement for award of a Degree of Master of Science in Information Technology. I wish to request your participation in this research for approximately 10 - 15 minutes. The information requested is needed purely for academic research purpose and will therefore be treated with utmost confidentiality. Kindly provide your responses as guided. Thank you in advance.

Please check for prompts or directions before responding to each questionnaire and/or section.

SECTION A: PERSONAL INFORMATION

1	**Name**				
2	**Institution-Organization genre e.g. Fintech, IT**				
3	**County**		**1.4**	**District**	
4	**Village/Ward**		**1.6**	**Gender**	☐ **Male** ☐ **Female**
5	**Department/Unit Size**				

SECTION B: COMPANY PROFILE

6) What is the name of the institution you work with?

_____

7) What is your current job title in the organization?

_____

8) What's your age? Or which age bracket do you fall in?

   a) Above 15 – Below 21 [ ]

   b) Above 21 – Below 31 [ ]

   c) Above 31- Below 41 [ ]

   d) Above 41- Below 51 [ ]

   e) 51 and Above [ ]

9) How long have you been with this organization?

   a) Less than 5 years [ ]

   b) 5 to 10 years [ ]

   c) 10 to 15 years [ ]

   d) 15-20 years [ ]

   e) More than 20 years [ ]

10) Which department do you work in?

   a) Human Resource [ ]

   b) Finance [ ]

   c) ICT [ ]

   d) Administration [ ]

   e) Support [ ]

   f) Other [ ]_____

11) Do you use personally owned devices e.g. Cell Phone/Smartphones, PDA/Tablets, Laptops, POS in carrying out company or organizational (corporate) duties?

a) Yes [ ]

b) No [ ]

12) If yes in questions 6 above, which devices do you use carrying out or undertaking your duties? Select all that apply.

i. Laptops [ ]

ii. Tablets [ ]

iii. Smartphones [ ]

iv. Pont of sales (POS) [ ]

v. Other (*specify*) [ ] _____

13) If No to questions 6 above, why?

_____

14) Are you aware of the organization's Bring Your Own Device (BYOD) security policy?

a) Yes [ ]

b) No [ ]

SECTION C: BYOD AND EXTENT OF USE

15) Select the choice that mostly illustrate your opinion given the scale below by ticking the corresponding box (*Tick appropriately*)

No.		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					
2.	It's okay for me to connect to the office network using the device in the office?					
3.	I am able to remotely (when out of office) connect to the office network using my device?					

16) Do you have device security applications in your devices?

a) Yes [ ]

b) No [ ]

17) If yes, which ones?

_____

18) If no, why don't you have?

a) Don't know any security applications

b) Don't think the security applications can help make my device secure

c) They are expensive

d) Don't trust the applications

e) Other (Specify) _____

19) Who do you contact in case of security issues?

a) My line manager

b) IT staff in the organization.

c) My colleague

d) My immediate neighbor

e) Anyone in the organization with a device

f) Those with similar security issues

g) Other (Specify) _____

20) Which of the following security solution(s) have you or the organization implemented in the secure adoption of BYOD concept in your organization? (*Select all that apply*)

No.	**Solution**	**Tick**
1	Mobile Device Management	
2	Mobile Application Management	
3	Mobile Information (Content) Management	
4	Mobile Identity Management/Identity and Authentication Management	

SECTION D: UPTAKE AND UTILIZATION OF THE PROPOSED IDENTITY AND ACCESS MANAGEMENT BYOD SOLUTION

The use and benefits of BYOD within organizations cannot be underscored. We thus need to grant access to manage devices, application, information and authenticate device users to achieve the main security services an operate in a more secure mobile environment.

21) Select the choice that mostly illustrate your opinion given the scale below by ticking the corresponding box (*Tick appropriately*)

No.	Choice	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	User identification and authentication should be incorporated in secure BYOD adoption					
2.	The proposed solution will result to value addition in the security architecture					
3.	The proposed solution is implementable					

22) What challenges do you think are faced or (are likely to be faced) by the organization which decide to adopt and implement 'Identity and Authentication Management' solution?

_____

_____

23) Specify any other strategy that you think should be employed in enhancing effective adoption of secure BYOD concept in your organization?

_____

_____

FOR MANAGEMENT AND DECISION MAKERS IN THE ORGANIZATION

SECTION E: BUSINESS VALUE TO ORGANIZATION

1) What measures has been put by the organization to secure devices and access to corporate resources?

_____

_____

2) On a scale of 1-5 how would you rate the security solutions implemented in your organization on the following areas (**1 being lowest and 5 being the highest**)

No.	**Area**	**1**	**2**	**3**	**4**	**5**
1.	Mobile Device Management					
2.	Mobile Application Management					
3.	Mobile Information (Content) Management					
4.	Mobile Identity and Authentication Management					

3) What choice among the below-provided, mostly illustrates your opinion whether BYOD implementation will lead or has led to the following business values/benefits given the scale? (*Tick appropriately the corresponding box)*

No.	**Values**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
1.	Increased efficiency					
2.	Increased profitability					
3.	Reduced Total Cost of					

	Ownership					
4.	Quick response time					
5.	Improved service delivery					
6.	Improved employee satisfaction					
7.	Improved and timely delivery					
8.	Social-economic benefits					
9.	Competitive advantage					
10.	Behavioural change					
11.	Improved coordination					

Thank you for taking time to participate & we look forward to share the findings with you.

Appendix B: Interview Guide for Top Managers

Dear respondent,

Hi, my name is…….. and I wish to request your participation in this research that will take between 10 - 15 minutes. The information requested is purely for academic research and will therefore be treated with utmost confidentiality. Your participation is voluntary and in case you feel some information is sensitive or you are not able to answer then you are allowed to 'not answer it/them' or keep quiet (pass). Your participation is highly appreciated and I kindly ask for your help in providing appropriate responses as guided. Thank you in advance.

(Provide the proposed solution info here)

1) Do you have a security policy or strategies that are used in the implementation of emerging technologies such as BYOD?

   _____

   _____

2) What challenges will you face in the implementation of the proposed solution in your organization?

   _____

   _____

3) In cases of security breaches who is or will always be held responsible?

   _____

   _____

4) In your own opinion, do you believe implementing BYOD and the proposed solution/measures affect productivity? Ease of use? Scalability? Cost effectiveness? Explain further,

   _____

   _____

5) Which features/functions should be integrated to assist in the improvement of the proposed identity and authentication management system?

_____

_____

6) Any other information or anything you would like to say about the proposed solution, the research or questions asked?

_____

_____

Thank you for taking time to participate.

Appendix C: Usability Testing Questionnaire

Identity management and User Authentication Usability Testing

1) Were you able to register a new user? *
   a) Yes [ ]
   b) No [ ]
2) If your above answer is 'No', kindly list the problems you encountered

   _____

   _____

3) Was the system able to send a Random Code notification to the device owner's phone? *
   a) Yes [ ]
   b) No [ ]
4) If your above answer is 'No', kindly list the problems encountered

   _____

   _____

5) How would you rate the whole application? Select an attribute (Number) that applies for each *.

Attribute	**1**	**2**	**3**	**4**	**Option Selected**
User Friendly*	Simple	Moderate	Somewhat complex	Complex	
Responsiveness*	Excellent	Very Good	Good	Fair	
Useful and Satisfying*	Strongly Agree	Agree	Neutral	Disagree	
Ability to Achieve Core Functionality*	Excellent	Very Good	Good	Fair	
Acceptability*	Accepted	Not sure	Accepted with reservations (only if certain conditions are met)		

6) What feature interested you most in the application *

_____

_____

7) Any comments, suggestions, or recommendations about this application

_____

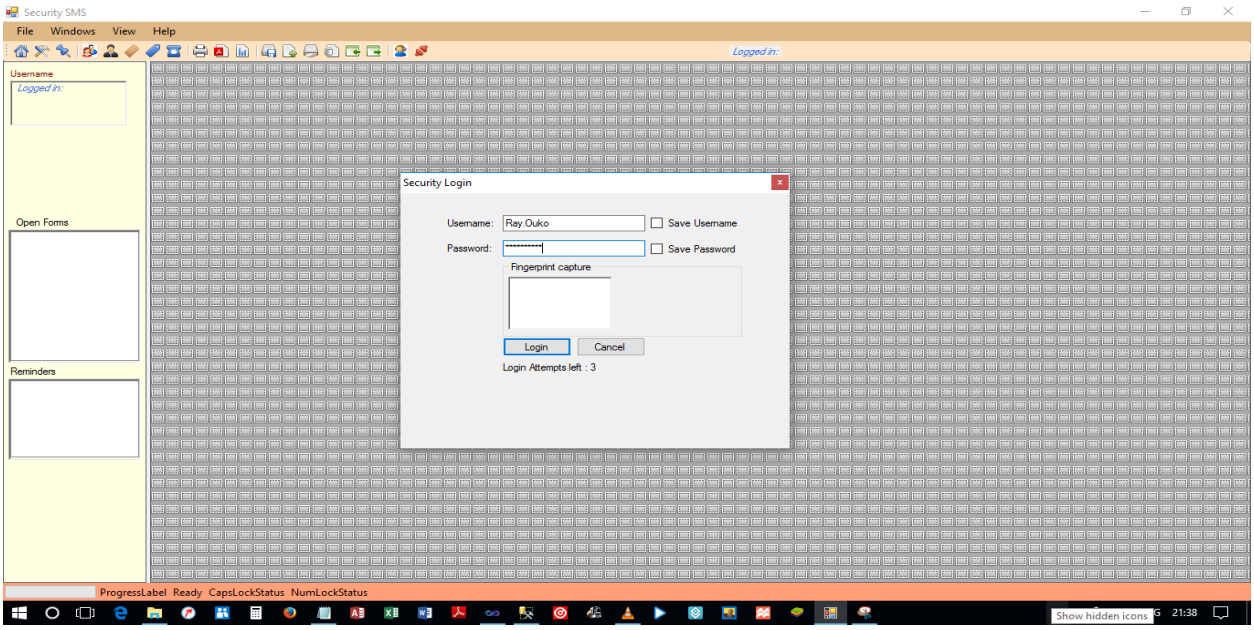
_____

_____

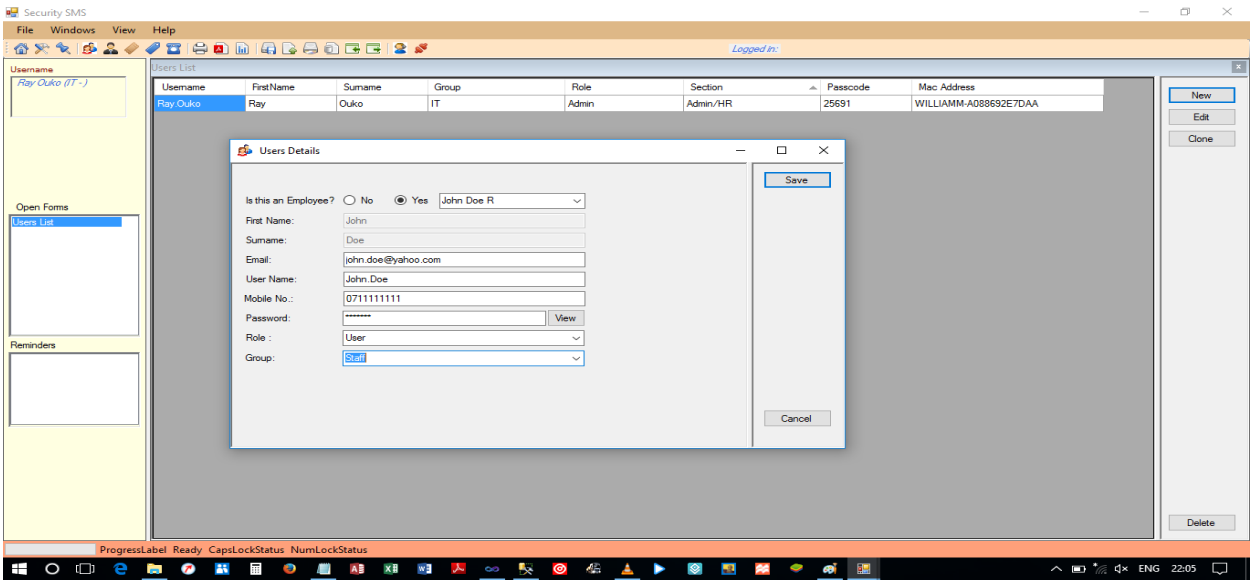
Thank you for taking time to participate.

Appendix D: Application Screenshots

The security login window allows registered users to provide their verification credentials (username and password/fingerprint combination) for validation as part of the log in process.



As indicated in Chapter 5, this window shows the system administrator's dashboard which part of the systems backend. It enables the administrator to perform certain actions such as; view full list of registered system users, edit their details whenever a user requests and deactivate/delete users whenever necessary.



Appendix E: Turnitin Report

Turnitin Originality Report

Device Identity Management and User Authentication by Ray Ouko

From 2016 Plagiarism Check (UG) (Library Services Plagiarism Checker (2016+))

- Processed on 06-Apr-2017 5:33 PM EAT
- ID: 795346901
- Word Count: 16101

Similarity Index
27%
Similarity by Source

Internet Sources:
21%
Publications:
7%
Student Papers:
20%

sources:

1 2% match (Internet from 26-Jun-2014)
http://ijsse.org/articles/ijsse_v1_i11_534_546.pdf

2 2% match (student papers from 16-Mar-2015)
Submitted to Strathmore University on 2015-03-16

3 2% match (Internet from 04-Nov-2012)
http://scholarsbank.uoregon.edu/jspui/bitstream/1794/12254/1/Emery2012.pdf