2017

A Mobile application for administering access control on mobile devices

Michael Muriithi Wanyoike
Faculty of Information Technology (FIT)
Strathmore University

A Mobile Application for Administering Access Control on Mobile Devices

Muriithi Michael Wanyoike

Submitted in partial fulfilment of the requirements for the award of a Master of Science in Mobile Telecommunication and Innovation (MSc.MTI) at Strathmore University.

Faculty of Information Technology

Strathmore University

Nairobi, Kenya

June, 2017

Declaration and Approval

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.

Muriithi Michael Wanyoike

…….....

June 2017

Approval

The dissertation of Muriithi Michael Wanyoike was reviewed and approved by the following:

Dr. Bernard Shibwabo,

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

Acknowledgement

I would like to acknowledge my supervisor Dr. Bernard Shibwabo who offered guidance and support throughout the research period. I would like to thank @iLabAfrica, Safaricom Academy and Strathmore University for the opportunity to do my masters' in their program and the exposure I got on my professional field. I would also like to thank my family for their continued support and encouragement and also I acknowledge the efforts of my mentors Emmanuel Muhanga, Hove Ebayi and Anne Mundati for their crucial role in offering support and guidance throughout the masters' period. Finally I thank the Almighty God for good health, favour and grace throughout these period.

Abstract

Mobile phones have become an integral part in our daily lives where services are now being offered through mobile applications. These applications rely on the mobile phone's local storage to store application specific data and also user data. This results to sensitive data ranging from personal data to corporate data being stored on the mobile phones which need to be protected from unauthorised people in case of malicious people trying to access sensitive data, theft or misplacement of the mobile phone. Control on the access of these sensitive data needs to be taken into consideration.

This research is aimed at finding the different types of access control mechanisms and which one will be best suited for a mobile device by determining the features that need to be included in order to provide a comprehensive secure access control mechanism. Therefore, this led to the development of a mobile application that aims at preventing unauthorised users from accessing sensitive data on the mobile phone.

The development of the application was achieved using the Agile Software Development Methodology since it provides a more flexible approach with the changing needs of the user and to easily add new functionalities whenever they are identified. This methodology eased the process of user acceptability as the user was involved in the development process. Testing and validations of the final system was done to ensure the solution solves the problems specified in the research.

Keywords: Access, Control, Secure, Mechanism, Sensitive, Data, Mobile Application

Table of Contents

List of Figures

List of Tables

Abbreviations

CPU	-	Central Processing Unit
DAC	-	Discretionary Access Control
HTML5	-	Hypertext Mark-up Language Revision 5
IT	-	Information Technology
MAC	-	Mandatory Access Control
OS	-	Operating System
PC	-	Personal Computer
PHP	-	Hypertext Pre-processor
PIN	-	Personal Identification Number
RAM	-	Random Access Memory
RBAC	-	Role Based Access Control
RB-RBAC	-	Rule Based Access Control
USB	-	Universal Serial Bus

Chapter 1: Introduction

1.1 Background

The popularity of smartphones is increasing with an increase in the services being offered through the Internet. According to Poushter (2016), the ownership of smartphones in developing countries is rising exponentially experiencing an increase of 16% from 21% in 2013 to 37% in 2015. The need for flexibility in communication and simplifications in how we carry out our daily routines has tremendously impacted the over reliance of smartphones in our daily lives. Increased computing power of smartphones has greatly influenced the growth of smartphones where the sales of smartphones have been way much higher than those of desktop computers since 2010 (Chen & Sivakumar, 2005; Penwarden, 2016; Fawcett, 2014; Shebaro et al., 2015).

The capability of smartphones to perform similar tasks as desktop computers has resulted to organisations adapting the use of smartphones in their operations for both their clients and their staff. The use of smartphones offers a cost friendly approach to organisations but majorly the most expensive aspect for any organisation is data. Smartphones phones can easily get hacked, lost or stolen and this proves to be a risk to the organisation (Perelson & Botha, 2004; Shebaro et al., 2015; Boyles, et al., 2012). The owner of the smartphone also risks to lose personal data which demonstrates a major bridge on privacy. Organisations offering their services through mobile applications together with social media applications make smartphone users end up with a junk of confidential data stocked up in their mobile phones (Boyles et al., 2012).

Existence of confidential data gives rise to the need for controlling the access to these data. In most computing environments, access control is used as the security technique to manage and control individuals that can make use of resources (Rouse, 2014). Access control is categorised into the physical and logical which mainly defines a comprehensive security model of a system. Physical access control is used to selectively limit resource access to individuals which mainly involves the use of authentication mechanisms. On the other hand, logical access control ensures connection limitations on networks, system files and data. For smartphones in particular, both the physical and logical security aspects must be taken into consideration so as to ensure data security irrespective of the device landing in the wrong hands (Poushter, 2016; Rouse, 2014; Perelson & Botha, 2004; Penwarden 2016).

The need for implementing access control is not only to secure confidential data but also to prevent exposing personal and sensitive information to the wrong individuals and preventing useful user content from being messed up. Parents will want their children to use their mobile phones but restrict access to certain applications and files. This aspect has led to the rise in parental control systems on mobile devices which purely utilise physical access control mechanisms so as to prevent children from accessing explicit content or being addicted to mobile phones.

1.2 Problem Statement

Overreliance of smartphones in our day to day activities has resulted to transfer and storage of highly confidential and personal data in smartphones. Loss of a device or unauthorised individuals having access to these devices can lead to infringement of privacy, exposing confidential information such as passwords and inappropriate content being easily accessible (Cooney, 2012).

Data stored in smartphones is confidential and should only be accessible to authorised users. Parents who let their children use their phone may expose harmful content to children through application data or may put useful user content in applications at risk of being messed up by children. Most phone owners do not implement any security feature in the smartphones but only depend on the inbuilt security features. This is mainly due to the perception that smartphones are secure but cases of hacking and unauthorised access of applications and data on smartphones are rising (Myhrvold, 2012). Few users with a rough knowledge in IT will proceed with adding additional features such as authentication before accessing mobile phones (Cooney, 2012).

Current systems have provided security through the use of authentication but this cannot single handedly be used as the only security mechanism. Connecting the device to a computer via USB will still expose all the application data, system files and any other data stored in the smartphone's storage. This proves that not only one mechanism can be used to provide a secure system.

1.3 Aim

The aim of this research is to develop a mobile application for smartphone users to protect their devices through a mechanism of blocking specific applications and also blocking the storage files of these applications in the smartphone so as to ensure any form of confidential data is not

open to unauthorised individuals. The mobile application will also utilise standard security features to secure transfer of personal information via the Internet.

1.4 Research Objectives

(i) To determine the challenges of administering access control on mobile devices.

(ii) To review existing methods used in administering access control on mobile devices.

(iii) To design, develop and test an access control mobile application.

(iv) To validate the mobile application to ensure it protects data for smartphone users.

1.5 Research Questions

(i) What are the challenges faced in administering access control on mobile devices?

(ii) What existing techniques and mechanisms are used to administer access control on mobile device?

(iii) How can a mobile solution be developed that will ensure administration of access control on mobile devices?

(iv) Does the developed application ensure Smartphone users control the access of data stored in their Smartphones?

1.6 Justification

In order to reduce unauthorised access to mobile applications and data stored on mobile phones, there is need to implement access control mechanisms to verify the person accessing the phone and to determine what is to be accessed to the authenticated users. Children often have access to their parent's phone which can expose them to harmful content or they might end up messing up with useful user content in mobile applications. Parents need to give access to their children but ensure that they control what they can access. There is only need to show to children what is relevant to them when they use the parent's phone while other applications and settings must be hidden.

Unauthorised access can also occur when the phone is stolen or close friends and family snoop through your phone. They can further access the phone storage files through USB connection to a PC in case an access control feature such as password authentication is configured.

Using a mobile application that will ensure the phone owner can control access of all features on the phone will enforce better security on application and data stored on mobile phones. Consequently, this will prevent exposure of harmful content to children, infringement of privacy through unauthorised individuals having access to private and confidential information and criminal offences such as access to banking applications.

1.7 Scope and Limitation

This research targeted Nairobi County. This region contains individuals who use mobile phones on a daily basis and the result obtained from this sample group provided the expected results that will represent similar outcomes in other counties. This study was limited to the Android platform since it boasts the majority of the market share. Future releases will include support for all the other platforms.

Chapter 2: Literature Review

2.1 Introduction

According to Perelson and Botha (2004), we are living in an era that is heavily influenced by digital technologies where mobile phones are becoming multi-purpose devices ranging from storing large data and running custom applications. This is evident as people are using mobile phones for personal use and business tasks which leads to data being stored locally on the phone. Therefore, the need to control access of these stored data becomes vital as it proves to be confidential to the owner of the phone or the organisation that owns the custom applications (Perelson & Botha, 2004; Chen & Sivakumar, 2005; Fawcett, 2014; Penwarden, 2016; Boyles, Smith, & Madden, 2012).

The need for access control influenced the aim of this study which was to identifying the different ways access controls have been implemented on mobile phones and to determine the necessary procedures in developing an application that will produce effective results based on the existing applications.

Therefore, this chapter discussed access control in detail and explained how different mobile phone operating systems support different aspects of access control. Thereafter, a discussion on the existing solutions was done with an aim of identifying gaps and solving the problems stated in our research questions and the effectiveness of the current solutions in meeting their goals. A comparison of the existing solutions with the proposed solution was carried out so as to determine the additional features that were to be added in the proposed solution. Finally, a discussion followed to ensure that the proposed solution is efficient and effective.

2.2 Access Control

Access control refers to the security features and mechanisms that are used to prevent restricted individuals from accessing certain system resources. In order to grant the right level of permission to an individual, different access control models are used depending on the organisations or user's preference (Chen & Sivakumar, 2005; 'InfoSec Resources - Access Control', 2012; Shebaro et al., 2015). The following section expounds on the different access control models.

2.2.1 Access Control Models

2.2.1.1 Mandatory Access Control (MAC) Model

According to 'InfoSec Resources - Access Control: Models and Methods' (2012) MAC model ensures that the end user does not have control over the access rights. These model normally has two levels which includes defining the rights and enforcing the defined rights. In most cases the system administrator is the person who defines the rights which are strictly enforced by the security kernel or the OS (Rouse, 2013; Watson, 2013). The rights are normally classified into confidential, secret and top secret where each user and device is assigned a classification and a clearance level. The classification and clearance level are used by the OS or security kernel to grant access to the user or device. The MAC model is the most secure model but it requires the repositories for the classifications and clearance levels to always be up to date (Rouse, 2013; Watson, 2013; 'MAC', 2014).

2.2.1.2 Role Based Access Control (RBAC) Model

RBAC model handles access control through roles that individuals are assigned in an organisation. RBAC works by assigning permissions to a role then the role is assigned to an individual instead of directly assigning permissions to an individual. The major issue with this model is that it is impossible to handle different access rights for individuals having the same role (House, 2005; 'InfoSec Resources - Access Control', 2012).

2.2.1.3 Discretionary Access Control (DAC) Model

According to 'InfoSec Resources - Access Control' (2012), MAC is the most restrictive access control model since the end user is limited to the rights set by the system administrator. DAC provides flexibility on the end user's access rights by allowing users have complete control of the objects and resources they own. This means that the end user is given complete rights to set security levels settings for other users on how they can access and use resources. These results to users having higher privilege than required which poses as a security loop hole. The DAC model also poses a great risk since the permissions and rights are inherited in other programs which gives leeway to viruses and malware running due to the high privileges granted to the end user ('InfoSec Resources - Access Control', 2012; Watson, 2013; 'DAC', 2014; Schneider, 2012).

2.2.1.4 Rule Based Access Control (RB-RBAC) Model

RBAC ensures that resources can only be accessed based on the set of rules defined by the system administrator. This model makes use of access control list similar to the DAC model which is normally associated with every resource object. These rules cannot be altered by the end user which provides high level security. The rules set in the access control list of a resource or object is used to guide the OS on whether to grant permissions for the user to access that resource ('InfoSec Resources - Access Control', 2012; Brachman, 2006).

2.2.2 Access Control and other Security Services

According to Perelson and Botha (2004) mobile phones form an integral part in most information sharing systems as they are currently being used to conduct business and personal tasks. For any information sharing system, security services have to be put in place. Access control forms part of the security services which is supported by four other services. These services include authentication, confidentiality, integrity and non-repudiation which are the basic principles of cryptography ('InfoSec Resources - Access Control', 2012; Fawcett, 2014; Arora, 2012).

The main aim of cryptography is to form strong encryption methods but encryption alone will not solve all data centric security issues. This is the main reason why Perelson and Botha (2004) explain a comprehensive security approach of combining the five security services. The authentication service is used to confirm the identity of the claimed user using predefined rules. Confidentiality services ensure that information is not disclosed to undesired individuals. Integrity services ensure that information does not change or get corrupted when accessed by undesired individuals. Non-repudiation services confirm and prove the source of the received information. In most cases it is used to ensure communication is carried out from the desired source. Access control services are dependent on authentication, confidentiality, integrity and non-repudiation service since it is the services that grants rights to authorised users and it requires all the these services to be functioning as desired (Perelson & Botha, 2004; 'Role of Cryptography', 2012; Arora, 2012;).

Perelson and Botha (2004) stress that all these services are interdependent which is evident in how the access control service works. This service needs an authenticated user and it will make use of the confidentiality service to ensure only authorised users have the right to access information. These interdependence is beneficial when aiming to implement access control on

mobile devices since a combination of any of the discussed services can lead to a good implementation (Perelson & Botha, 2004; Perrin, 2007; Newton, 2014).

2.2.3 Access Control Features

The previous section has discussed on the services that are used together with access control service to come up with a better secure system. According to Perelson and Botha (2004), the features that exists in these services can be combined to come up with a secure access control on mobile devices. The features of these services can be summarised under authentication and authorisation services (Perelson & Botha, 2004; Gaur, 2015, 'Security Access Control', 2013). Figure 2.1 outlines the features under authentication and authorisation.

Authentication	Authorisation	Other
Passwords	File masking	Encryption
Biometrics	Access Control Lists	Synchronisation
Auto Logout	Role-Based Access Control	

Figure 2.1: Security Services and Related Features for Access Control (Adapted From Perelson & Botha, 2004).

2.2.3.1 Authentication Features

Perelson and Botha (2004) classify passwords, biometrics and auto logout as features under Authentication. These features handle how system users are allowed access to the system. For instance, passwords are unknown values only known by the user that ensures precise authentication of the user. Only users with the correct password can access the system. On the other hand, biometrics ensure authentication is carried out using the physical attributes of a user where a distinct hardware device is needed to get the user's input. The auto logout is a feature that terminates a session or logs out the user after a period of inactivity. This period is usually set by the system administrator (Perelson & Botha, 2004; Shinder, 2001; Miessler, 2005; 'Security Access Control', 2013; Gaur, 2015).

2.2.3.2 Authorisation Features

File masking, access control lists and role-based access control are some of the features classified under authorisation. File masking is a feature dependent on user authentication which

involves the system preventing access or viewing of certain resources before authenticating the user. Access control list apply a similar principle as file masking but now a list of users are given access rights to certain objects or resources mainly through permissions that are outlined in the form of a matrix. Role based access control implement the principle of access control lists by creating roles and associating roles with specific users. These roles are assigned access rights and permissions to specific objects therefore resulting to access rights being based on a certain role (Perelson & Botha, 2004; Gaur, 2015; Shinder, 2001; House, 2005; Sattarova Feruza & Kim, 2007).

2.2.3.3 Other Security Features

Perelson and Botha (2004) found features that could not be classified under authentication or authorisation but still prove vital features for a secure system. Encryption and synchronisation are among the important features where encryption involves mechanisms that make use of cryptography to ensure data is secure. Synchronisation involves the mechanisms used for backup, restoration and ensuring the user accesses the current data (Perelson & Botha, 2004; Cha, 2016; Messer, 2017).

2.2.4 Access Control on Mobile Devices

Access control on a mobile device involves the user of a mobile device being activated and authenticated based on a password or biometric measure (Perelson & Botha, 2004; Shinder, 2001; 'Security Access Control', 2013). The basic process of access control in mobile devices is shown in Figure 2.2.

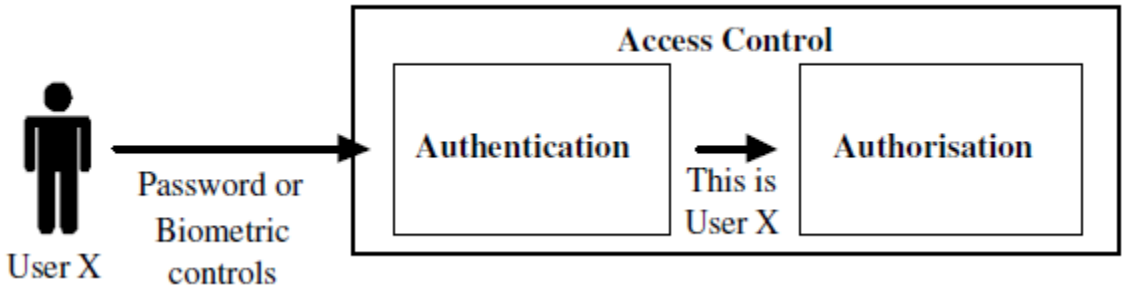

Figure 2.2: The Process Flow Towards Access Control on Mobile Devices (Adapted from Perelson & Botha, 2004).

Perelson and Botha (2004) stress that not all access control features discussed in the previous section are available in all mobile devices. These features are dependent on the mobile device manufacturer's preference and the technology, both software and hardware, required to support a specific feature. Such differences are evident when investigating features between iPhone and Samsung which are the leading mobile phone manufacturers (Perelson & Botha, 2004; Forrest, 2016).

Normally access control is implemented as a modular design in mobile device operating systems which makes it easier for mobile device manufacturers to select the operating system features the need to implement. All mobile device operating systems have the basic features of authentication and encryption mainly used to authenticate the user and encrypting application data or for secure communication purposes (Perelson & Botha, 2004; Cha, 2016; Singh, 2004).

Other access control features may differ in how they are implemented in different mobile operating systems. Figure 2.3 displays a summary of the features that exist in different mobile operating systems.

	Pocket PC & Smartphone	Symbian OS	Palm OS	J2ME
Passwords	✔	✔	✔	✘
Biometrics	✔	✘	✔	✘
Auto Logout	✔	✔	✔	✘
File Masking	✘	✘	✔	✘
Access Control Lists	✘	✘	✘	✘
Role-Based Access Control	✔	✘	✘	✘
Encryption	✔	✔	✔	✔
Synchronisation	✔	✔	✔	✘

Figure 2.3: Availability of Features in Different Mobile Platforms (Adapted from Perelson & Botha, 2004).

Based on the analysis of access control features between different mobile platforms, there are that gaps exist in the access control features of the listed mobile operating systems as shown in Figure 2.3. The reason for the inexistence of certain features in mobile operating systems maybe due to omissions by the mobile device manufacturer due to the computing power of the devices.

A good example is how strong encryption is not implemented on most mobile devices since they are processor intensive resulting to manufacturers opting for weaker encryption techniques. Only current Smartphones have powerful processors and can easily perform processor intensive operations. Implementation of role-based access control and control lists features are features that his not present on mobile devices but will provide better mechanisms in handling access control (Perelson & Botha, 2004; House, 2005;).

2.3 Challenges Administering Access Control on Mobile Devices

2.3.1 Lack of Standards for Implementing Access Control

Standardisation of the different access control architectures needs to be done in order help device manufacturers select the best access control features for their devices. Lack of Standardisation leads to lack of trust in access control capabilities of mobile devices therefore affecting the implementation of access control features (Perelson & Botha, 2004). Standards ensure stable and tested methods and technologies are implemented and also aids in future proofing the current solution (Brandewie, 2009).

2.3.2 Managing Access Privileges

According to Brandewie (2009), is the most important aspect of an access control system. Privilege management involves managing what a specific user can access. Solomon (2013) explains that handling multiple user loggings in mobile phones is a challenging process since every user needs to be treated as having a unique protected account. Every action of a specific user is hardly a private affair which can be handled with proper management and implementation of access privileges (Solomon, 2013).

2.4 Existing Applications

This section will review applications that make use of any form of access control to achieve their main goal.

2.4.1 AppLock DoMobile App

AppLock contains features such as blocking applications and mobile services, photo and video vault and creation of profiles and hiding the icon for AppLock. Applications to be blocked are selected and can either be saved in a profile. The mobile phone owner can create a profile and specify the settings to be used for that profile. This creates an option for allowing a person to use

the mobile phone as a guest with minimal or no capabilities of making changes. A change to another profile requires the mobile phone owner to manually change it in the AppLock settings (‘App Review’, 2016).

Video and Photo vaults ensure pictures and videos are hidden from unauthorised people by removing them from the gallery but are still visible in the file manager. For security purposes, the AppLock Icon can be hidden from the application home screen or launcher and the backend of the application can only be accessed through dialling “#” followed by the set password (‘App Review’, 2016).

2.4.2 Bit Defender Mobile Security

Bitdefender is an antivirus application developed by Bitdefender. Apart from offering security from viruses and malware, it contains anti-theft, App Lock, web security and snap photo feature. The App Lock feature ensures a pin is placed on the locked application with any wrong authentication leads to the anti-theft feature being activated. This feature will make use of the snap photo feature by secretly taking the photo of the unauthorised person trying to access the application. Bitdefender also prevents installation of applications that prove to be a threat to your privacy (Rubenking, 2016).

2.4.3 DU Antivirus

According to Wells (2015) DU Antivirus contains features such as App Lock and private vault to prevent access to certain system resources. App Lock feature allows a user to lock al applications with just a single password. Any attempt to access the application with the wrong password will secretly take a photo of the intruder and compile the sequence of photos in a feature called the break-in alert. All photos will have a description of the application that was being attempted to be unlocked together with the date and the time (Wells, 2015).

The privacy vault feature ensures that photos and videos are hidden and encrypted which provides an added security level from the already existing App Lock. Other features such as the lock uninstall feature prevents unauthorised from on uninstalling applications especially DU Antivirus application which applies security bridges to other applications (Wells, 2015).

2.4.4 Funamo

Funamo is an application that provides comprehensive parental control for Android phones and tablets. Its main features include web filtering, device monitoring and application control. For its application control feature, parents are able to block protected apps and set time limits and time allowances for selected applications. It has a special device control feature where it blocks all the apps and makes the device go to sleep. Newly installed applications are quarantined which can only be used when authorised by the administrator.

In order to access a blocked application, the correct pin or authentication pattern must be input. Funamo contains other features such as device monitoring and web filtering for purposes of tracking the location of children and blocking websites respectively (‘Funamo’, 2015).

2.5 Research Gap

The process of offering access control to mobile devices has been well implemented in the existing applications. The aim to limit access to applications, videos and pictures to only authorised users. As discussed before there are different models of access control the most common one being Role-Based access control which is commonly used in organisations to manage the rights of every user. The existing applications have not implemented a dynamic way of allowing different user’s with different access rights to use the mobile phone.

AppLock developed by DoMobile managed to create different profiles but a single profile can only be used. A change to a different profile will require the mobile phone owner to make changes in the application settings. This proves to be a challenge in efficiently implementing access control on mobile devices. The need for the role-based approach is to create different user roles where each role has been assigned different privileges and access rights. Different users can access the mobile phone with the rights changing dynamically based on the role of the user.

Blocking an application creates an impression that also the application resources are blocked. Connecting the mobile phone to a computer via USB reveals access to all the application resources which demonstrates that there is a security gap in the whole process of trying to limit access to applications and its data. There is need to protect application data and resources stored in the mobile phones storage space so as to protect personal or organisation data in case of theft of the phone or malicious individuals.

AppLock has implemented a security feature of hiding the application's icon and using a secret code to access the application. The main aim is to prevent knowledgeable users from identifying the application being used for blocking applications. The main aim of this approach is to improve on security therefore it presents a better approach of how blocked applications should be handled when implementing another security layer. Blocked applications should not be shown to the normal user creating the impression that the application has not been installed. This ensures only the relevant information is shown to the user as specified by the mobile phone owner.

2.6 Conclusions

The need for access control is growing as people need to secure information stored in their phones and control the use of applications in their phone in cases where their phone is stolen or unauthorised individuals trying to use the phone. Current solutions are only providing features for blocking applications, videos and photos which proves not to be a comprehensive solution to implementing access control. These applications also do not handle different users based on their roles.

The proposed solution will aim to provide dynamic access control mechanisms through the implementation of a role-based access control model. Users with different roles will access a different profile depending on their roles and rights associated with that role. As discussed in this chapter, MAC model is the most secure since it offers a restrictive approach in how rights are assigned. The existing application will make use of both models where the phone user will act as the system administrator by creating roles and assigning rights to these roles.

The existing application will also aim to provide comprehensive security mechanism for data stored in the phone by blocking access to resources in the phone storage through USB connections to the computer. This will be a setting that can only be set by the phone owner who is the administrator in this case.

To improve on the security measures, the existing application will be implemented as a launcher application where only the allowed applications and settings will be displayed and this will dynamically change depending on the role of the authenticated user.

Chapter 3: Development Methodology

3.1. Introduction

This chapter outlines the methodology used by the researcher to achieve the research objective. A brief discussion on the stages of the research, location of the research, data collection techniques and development tools will follow.

3.2 Software Development Methodology

Agile development was the methodology used to carry out this research. This methodology is a combination of iterative and incremental processes with focus on process adaptability and end user satisfaction by progressively delivering a working software product (Shelly & Rosenblatt, 2012).

Agile methodology divides tasks into small time frames which aim to deliver specific features for release. The iterative approach ensures a software build is delivered at the end of every iteration. All these builds are always incremental in terms of features and the final build contains all the requirements from the client or all the features foreseen before development begun (Tutorialspoint, 2017). Figure 3.1 show the phases followed in agile methods in order to produce a working solution.

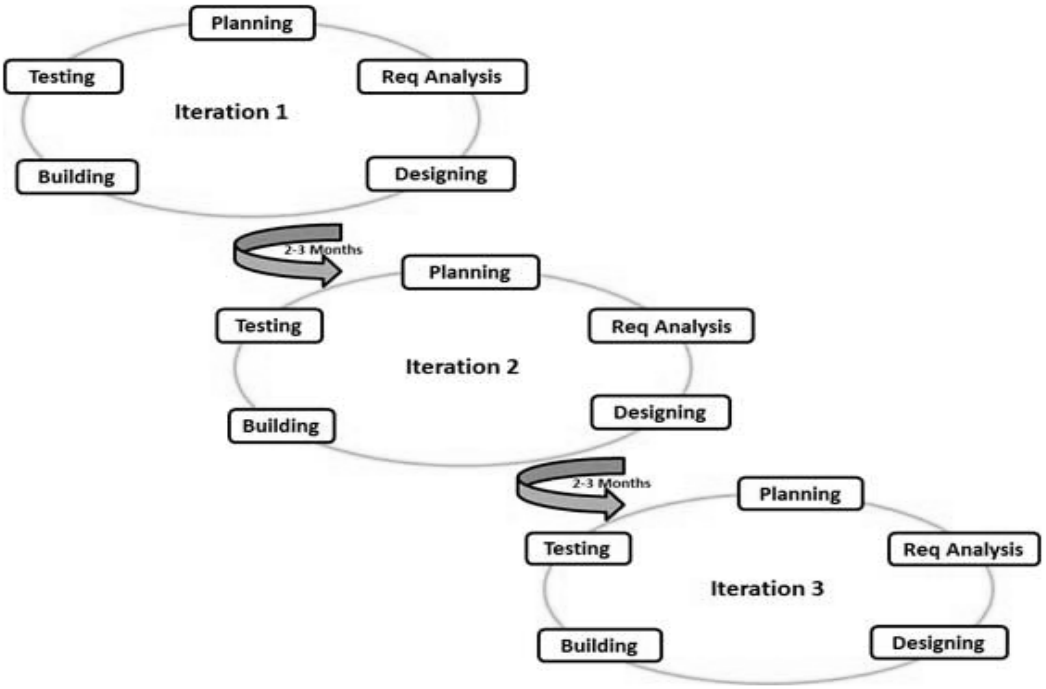

Figure 3.1: Steps in Agile Methodology (Tutorialspoint, 2017).

3.2.1 Planning Phase

This is the initial phase of the methodology which seeks to outline and facilitate how the entire process will be undertaken. Planning helps in identifying what resources will be needed to achieve or to build the system (Tutorialspoint, 2017).

3.2.2 Requirements Analysis Phase

This is the second phase which involves analysing the requirements of the system or what the system is expected to do. Analysis helped reveal important aspects of the system that was to be developed including the system users and the environment they were currently working on so as to determine what exactly the client wanted and what factors might have affected the development and testing of the application. For analysis to take place, data had to be collected from all the proposed system stakeholders. Consequentially, this presented a need of determining a sample size from the entire target population from which data was collected.

3.2.2.1 Sampling Strategies

Stratified random sampling was used to come up with the sample population. It involved creating smaller groups based on relevant attributes and selecting at random a sample from each group. This sampling strategy ensured people from specific subgroups were well represented within the sample space.

3.2.2.2 Sample Size

A total of 80 people were involved in this study where stratified random sampling was used to select the sample. The sample included different individuals in the social class so as to produce an accurate solution on access control on mobile devices. The sample size was determined through the use of the following formula.

$$Necessary\ Sample\ Size = (Z\text{-}score)^2 * StdDev*(1\text{-}StdDev) / (margin\ of\ error)^2$$

Z-score is the reading of confidence level from the Z-score table (Smith, 2013).The factors below had to be taken into consideration before determining the sample size.

i. **Population Size.** This entails the number of people that fit into the demography or the number of people that fit into the scope of the research that the researcher wanted to carry out. Smith (2013) explains that this number could be unknown or could be approximated.

ii. **Margin of Error (Confidence interval).** Smith (2013) suggests that no sample is perfect and there is need to know how much error can be allowed. Smith (2013) further explains that the margin of error entails how much higher or lower than the population mean the researcher is willing to allow the sample mean fall. This had to be determined before calculating the sample size.

iii. **Confidence level.** This was necessary so as to help determine how confident the researcher was that the actual mean fell within the confidence level (Smith, 2013).

iv. **Standard Deviation.** This is how much variance is expected in your response (Smith, 2013).

Researcher's confidence level was 0.89 z-score table reading

Standard deviation was 0.5

Margin of error was 0.05

Therefore, applying the above formula;

Necessary Sample size = (0.89*0.89) * 0.5(1 – 0.5) / (0.05 * 0.05)

=79.21 equated to 80 since u cannot have 0.21 of a person

3.2.2.3 Data Collection Process

Data collection was done to help identify the needs and the capacity of the target population so as to develop a better, usable and problem solving application. Information on access control on mobile devices was collected from respondents who included individuals from different social classes. This information was collected through the following methods:

i. Questionnaire

The questionnaire in appendix A was administered to respondents in the sample group which proved beneficial in understanding the situation on the ground and coming up with the requirements of the proposed solution.

ii. Observation

The researcher had to investigate the effect of lack of access control on mobile devices and used this observation as a source of gathering information.

ii. Document Review

This approach involved reviewing the existing techniques and mechanisms that are being used to implement access control so as to provide a more in depth knowledge on what earlier developments were done on the same line of research. The reviewed documents included, journals, academic documents and online articles on the techniques that various individuals and companies apply ensure data and application security on mobile phones.

3.2.3 Design Phase

The design of the solution followed after the requirements were analysed. The design included database design, use case diagram design, which showed all the actors and use case that they had, entity relation diagram and the system mock up designs. These designs were important because they guided the next phase which entailed the actual building of the system or development phase (TutorialPoint, 2014). The following diagrams were used in the design.

i. Use Case Diagram

Use case diagrams was used to identify the different actors in the system and how they interact with the system (Ambler, 2014b).

ii. Design Class Diagram

The class diagram was used to show objects in the system, their attributes or characteristics and their behaviour or functions. It will also show how these objects are related to each other and with what cardinality value (Ambler, 2014a).

iii. Entity Relation Diagram

The entity relation diagram showed various entities and their attributes of the system and how these entities relate together with their cardinalities (Shelly & Rosenblatt, 2012).

iv. Sequence Diagram

The sequence diagram was used to show interaction of the system objects (Bell, 2004).

3.2.4 Building Phase

This phase represents the actual implementation phase of the designs that were done on the previous phase (TutorialPoint, 2014). Design of mock-ups were turned into actual system windows which were fully functional. The database was created which made use of the Entity Relation Diagram where all the tables and their relations were included.

3.2.4.1 Prototype Development

Development of the solution will be done in phases. The first phase will involve development of the mobile application using Android programming followed by the development of the database using SQLite and MySQL. The final phase will involve development of the backend using PHP, HTML5, CSS 3 and JavaScript. Design frameworks such as bootstrap will be used to create attractive designs for the backend.

3.2.4.2 System Development Tools

i. Database development tools

For the development of the database, MySQL administrator will be used to develop the database. MySQL database is scalable and flexible since handles deeply embedded applications and can run data warehouses that hold terabytes of information. It allows customisation to add unique requirements mainly for a specific functionality. In addition to scalability and flexibility, MySQL database implements strong security features, have high performance in terms of meeting the most demanding performance requirements and 24/7 support despite being an open source database (‘Reasons to Use MySQL’, 2017).

ii. Programming tools

For the programming tools, Android studio will be used for Android programming, Adobe Dreamweaver CS5 for the design and development of the backend system. Android studio is an easy to use tool for developing Android applications with the desired packages readily available for download making it a better tool for Android programming.

3.2.5 Testing Phase

Testing will be done after completion of each build. This will aim at proving the objective of that build has been met. All types of testing will be done on the module of build or the system to ensure that it can withstand any eventuality (TutorialPoint, 2014).

3.2.5.1 Testing of the Prototype

Various types of tests will be carried out to ensure the prototypes meets the main objective and that it. The prototype will be tested for its functionality and user acceptance. The following are some of the tests that will be performed.

i. **Usability Testing-** This will be done to determine the usability of the application being developed. This will help check whether the application will be easy to use or what pitfalls would the users might come across. To achieve this, a total of 30 respondents will be sampled to test the application and give their response on the same.

ii. **Load Testing-** This will be used to check Big O notation of the application. This means checking the amount of time the application will take to process a request for instance loading a certain feature.

iii. **Integration Testing-** This involves testing the functionality of all the modules when combined ensuring there are no issues with the integration.

iv. **Functional Testing-** This will be done to test the whole system including the backend system.

3.2.6 Reasons for Adapting Agile Methodology

Agile is the best software development methodology to use in a dynamic environment with constant changes and new features required. This is due to its ability to quickly adapt to change and embrace continuous development (Tutorialpoint, 2015). Suggestion of new features or changes on the existing features during prototyping is a common phenomenon which agile methodology easily adapts to.

The aspect of introducing the user on board during the development process results to accurate user requirements that could not be identified during the requirement analysis phase. These result to the development of a solution close to what the user expected. Involving the user during development helps the user understand how the application works requiring little or minimal training when deploying the system.

3.3 Conceptual Model of Proposed Solution

The proposed solution made use of a role-based approach in administering access control. Different roles were created and access rights linked to specific roles. Users were assigned specific roles which determined the applications and settings that will be displayed to them. The application was implemented as an application launcher so as to take control of the activity of the whole phone. At this level access right were easily implemented where users had to enter their PIN in the lock screen window in order to access the application launcher. This ensured that the application authenticated the user and checked the access rights assigned to the user's role and

only displayed the allowed applications and settings. The phone owner performed administrative work through authenticating through the hidden administrator login screen. The login screen was accessible through a long press to the phone's home screen.

The proposed application also provides access control to the data stored on the mobile phone by preventing access through USB connections. The phone owner has a settings option of either allowing or preventing access to phone storage. Further the proposed solution has a backend for performing analysis and generating reports.

3.4 Conclusions

This chapter has described the methods and processes that were used to collect data and answer the research questions. Further discussions on the stages of agile methodology, sampling strategies, research design and system development tools were conducted.

Chapter 4: System Analysis and Design

4.1 Introduction

This chapter discusses system analysis and illustrates the system design components. System analysis involves requirement analysis which entails analysis data collected from the users of the system. System design involves showing a structure to how the proposed solution will be developed. This chapter will discuss these two aspects in detail with an aim of getting the requirements of the system and using these requirements to design the system.

4.2 Requirement Analysis

System requirements were gathered through the use of online questionnaires in the form of google forms. A total of 80 people were targeted to participate in the survey and the data was analysed using features of Google forms. 60 respondents successfully responded to the questionnaires. The response to this questionnaires helped answer some of the research questions and also played a big role in the design of the system. A sample of the questionnaire is attached in the Appendix A.

4.2.1 Functional Requirements

These are the functions which the system will perform in order to achieve the user's objective. After analysis of the requirements, the proposed system will perform the following functions:

i. Start application- This function will enable the user to start the application so that they can start using it.
ii. Create account- this function will ensure all phone owners register by setting up a username and password which will be used to access the system.
iii. Create other accounts- this function will allow phone owners create accounts to be used by different users.
iv. Delete Account- The phone owners must be able to delete all account.
v. Login- phone owners will be able to access the system by authenticating using their username and passwords. This function will only apply for registered administrators. Guest users will access the system using passwords generated by the phone owner.

vi. Block applications- This function will enable the phone owner to block specific applications on any account.

vii. Block data access- This function will enable the administrator to block phone data access through USB.

viii. Report on blocked applications and settings- This function will enable the phone owners to view a report on all the blocked applications and settings.

ix. Analyse blocked application- This function will enable the administrator analyse the category of applications blocked and further advise the phone owner on the applications they should likely block based on their existing settings.

x. Logout – All administrators must be able to logout of the system.

xi. Stop application- This function will terminate the application.

4.2.2 Non-Functional Requirements

These are the requirements that will not affect the main functions of the application. The application can function without these requirements but they are important in the final product of the proposed solution. The following are some of the non-functional requirements identified in the requirements analysis phase:

i. Performance- The application and backend must have a short response time when performing its functions and when responding to client requests respectively.

ii. Connectivity- the application and the backend system needs to be connected to Internet for them to be available and accessible at all times.

iii. Integrity- The data stored on the phone or transmitted to the server should not be altered or get corrupted.

iv. Reliability and availability- The system should always be available to perform user's task irrespective of errors and downtime.

v. Scalability- The system should be able to adjust well to user needs based by allowing features to be added.

vi. Usability- The system should be easy to use and users should use minimal steps to accomplish a tasks.

4.2.3 Demographics Data

Findings from the responses show 58% of the responses came from the male gender while 42% came from the female gender. In general, the youths dominated the responses where 74% of the respondents were youths and the remaining 26% shared among the older age groups as shown in Table 4.1. Out of the 60 responses, 70% were single and the remaining 30% were married. 60% of the respondents had attained a university degree, 22% had attended college and the remaining 18% attained a secondary school certificate.

Table 4.1: Demographics Statistics

DEMOGRAPHICS	FREQUENCY	PERCENTAGE (%)
Gender		
Female	25	42
Male	35	58
Age		
20 – 29	44	74
30 – 39	11	18
40 – 49	5	8
Marital status		
Married	18	30
Single	42	70
Highest level of education		
Primary	0	0
Secondary school	11	18
College	13	22
University	36	60

4.2.4 Mobile Phone Owners

Prior to implementing the proposed mobile phone solution, it is important to know how many people own a phone. Analysis from the respondent's response show that 85% of the

respondents owned a phone and only 15% did not own a phone at the time the survey was being conducted as shown in Figure 4.1. The reason for lack of owning a phone was largely due to phone theft and misplacement which constituted 99% of the reasons why the respondents did not own a phone and the remaining 1% was due to phone damages and repairs.

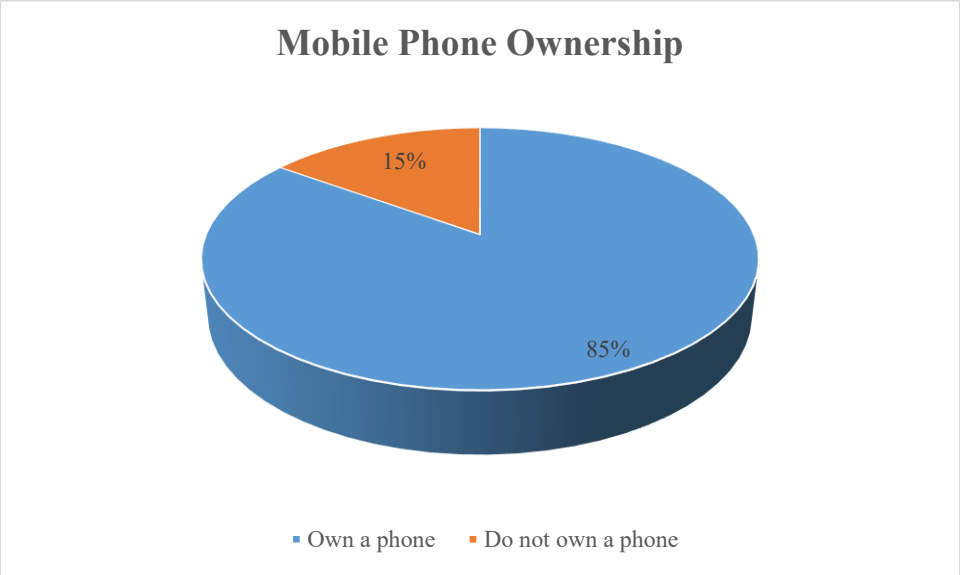

Figure 4.1: Mobile Phone Owners

4.2.5 Types of Phones

The proposed solution aims to provide a mechanism of controlling what application and data can be accessed by individuals who don't own the phone. In order to come up with an application that will meet this demand, there is need to know the market share of the different devices in the current market. This was done by enquiring from the respondents what type of devices they use and specifically which OS platform. 95% of the respondents claimed to be using smartphones with only 5% still using feature phones as their main mobile phones as shown in Figure 4.2. Out of the 95% who claimed they use smartphones, 20% of them still use feature phones reason being that they hold power for a longer time and easily serve as a backup to the smartphones.

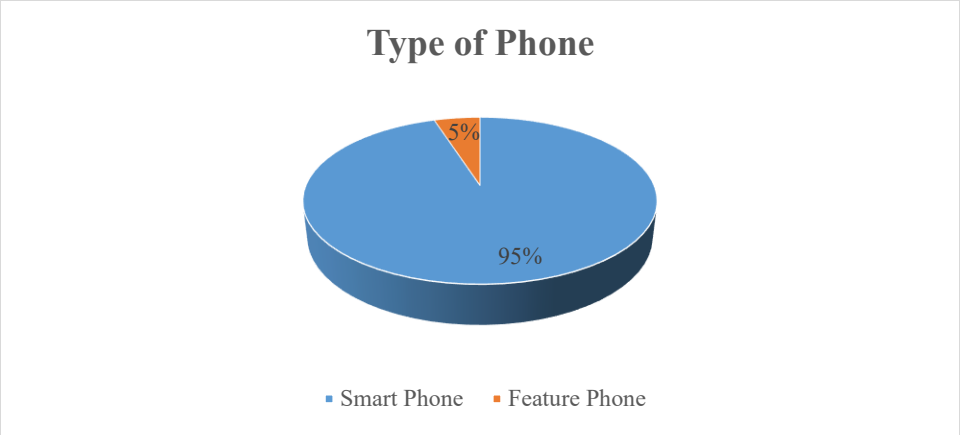

Figure 4.2: Different Types of Phones

4.2.6 Mobile Device Operating System Popularity

The previous section clarified that the solution to be developed must be for smartphones since they are the most popular among the respondents. There was also need to know from the respondents which operating system is utilised by their smartphones. Out of 60 respondents, 40 of them selected Android, 8 selected Blackberry OS, 5 selected iOS, 4 selected Windows Mobile and the remaining 3 respondents selected Symbian OS. Based on the respondent's response, it is clear that the Android platform is the most suitable for developing the application then later rollout to other platforms. Figure 4.3 shows a summary of the analysis of the popularity of operating systems.

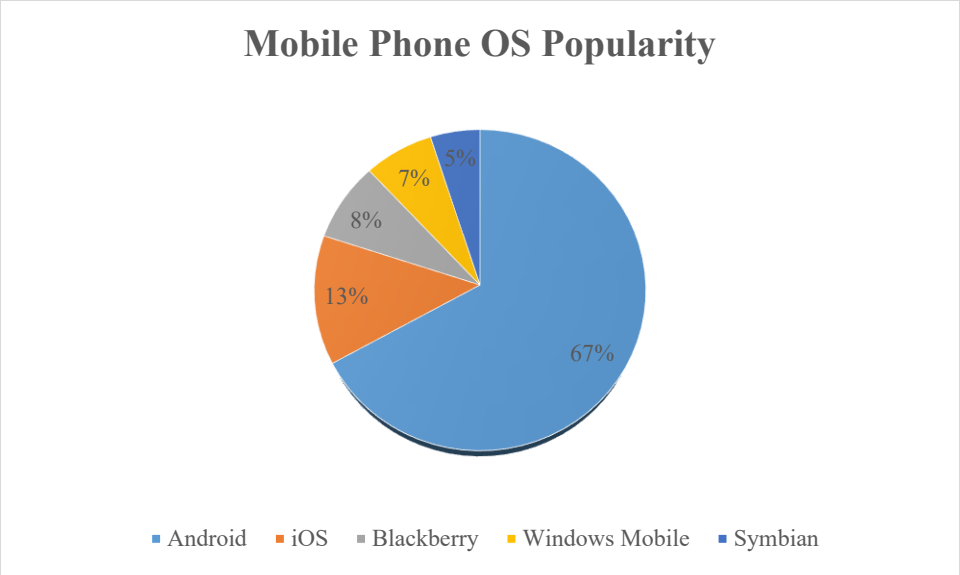

Figure 4.3: Most Popular Operating System

4.2.7 Awareness of Storage of Sensitive Data on Mobile Phones

The respondents were asked if they were aware of the storage of sensitive data on their mobile phones which could pose a risk to them if accessed by unauthorised individuals. 45 of the respondents (82%) said that they are aware of the storage of sensitive data that needs to be secured while 15 of them were not aware of the storage of sensitive data. Figure 4.4 shows a summary of the respondent's responses.

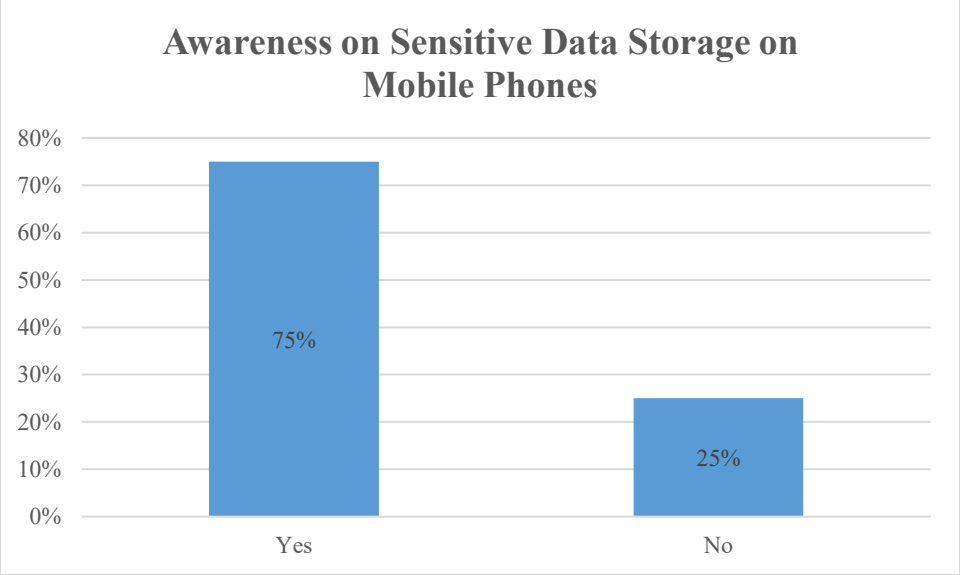

Figure 4.4: Awareness on Storage of Sensitive Data

4.2.8 Experience with Insecurity of Data Stored on Mobile Phones

In order to determine if a solution is needed, respondents were asked whether they have faced scenarios where they felt their personal data was unsafe. 96% of the respondents said that they have had concerns with the security of the data stored in mobile phones and the remaining 4% did not have any concerns as shown in figure 4.5. The 58 respondents who had concerns with the security of their mobile phones had to select the scenarios as to how they felt their data was not secure from a range of strongly disagree to strongly agree. The scenarios of data insecurity were:

i. Phone theft.
ii. Unauthorised individuals including friends, family and strangers using or snooping through the phone.
iii. Connecting phone to any computer via USB.
iv. Others.

Out of the 58 respondents that had concerns with the security of data, only 3 respondents selected other reasons on the above options which constitute 5% of the respondents who had concerns with the security of data. The remaining 55 respondents which constitute 95% of the sample responded to the scenarios outlined above as shown in Figure 4.6. Figure 4.7, figure 4.8 and figure 4.9 shows a summary of the responses.

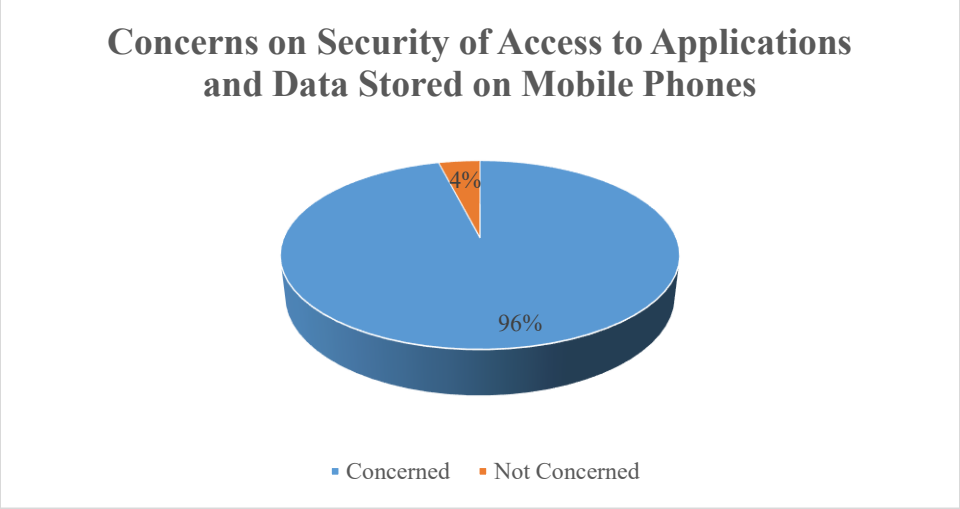

Figure 4.5: Concerns on Security of Access to Applications and Data Stored on Mobile Phones

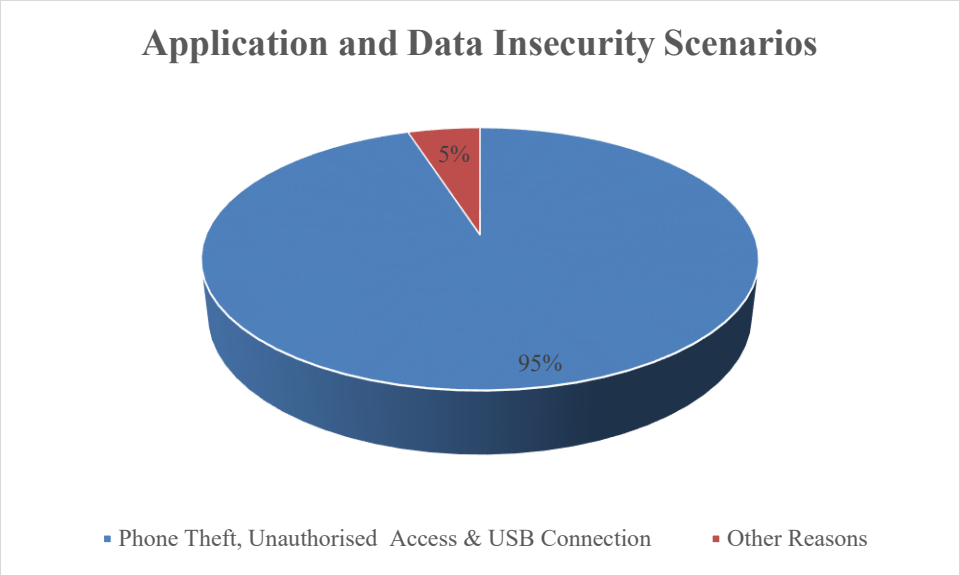

Figure 4.6: Respondent's Reaction to the Scenarios that Expose Data

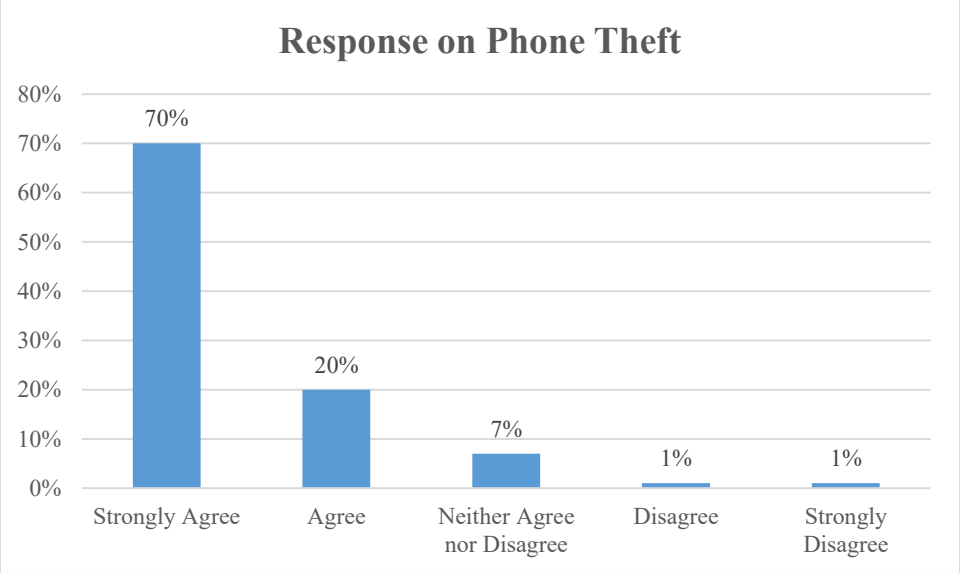

Figure 4.7: Respondent's Reaction to Phone Theft or Misplacement

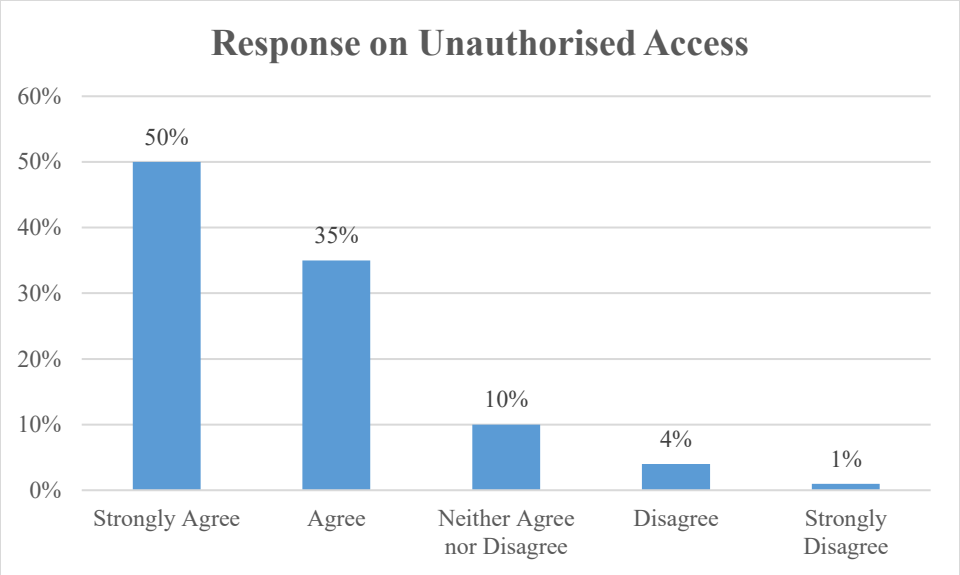

Figure 4.8: Respondent's Reaction to Unauthorised Access

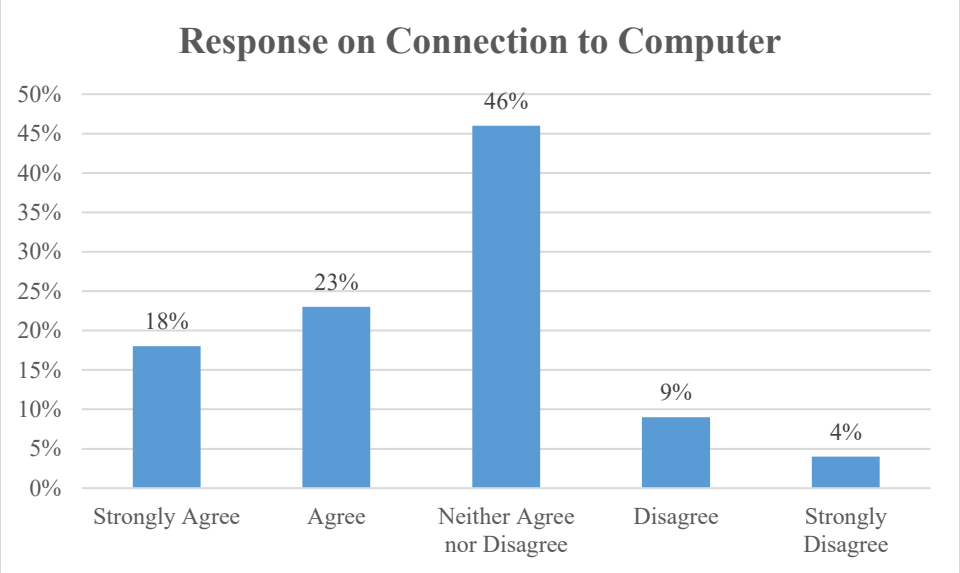

Figure 4.9: Respondent's Reaction to Connections to a Computer

4.2.9 Awareness of Technology Used to Protect Application and Data Access

The respondents were asked whether they were aware of any existing solutions that aim to protect application and data access. 42 respondents said they were aware of these applications and further gave examples and the remaining 18 respondents were not aware as shown in Figure 4.10. All of the 42 respondents mentioned antivirus applications and parental control applications. Out

of the 42 respondents, only 4 respondents knew of applications specifically designed to protect application and data access. Figure 4.11 shows a summary of this data.

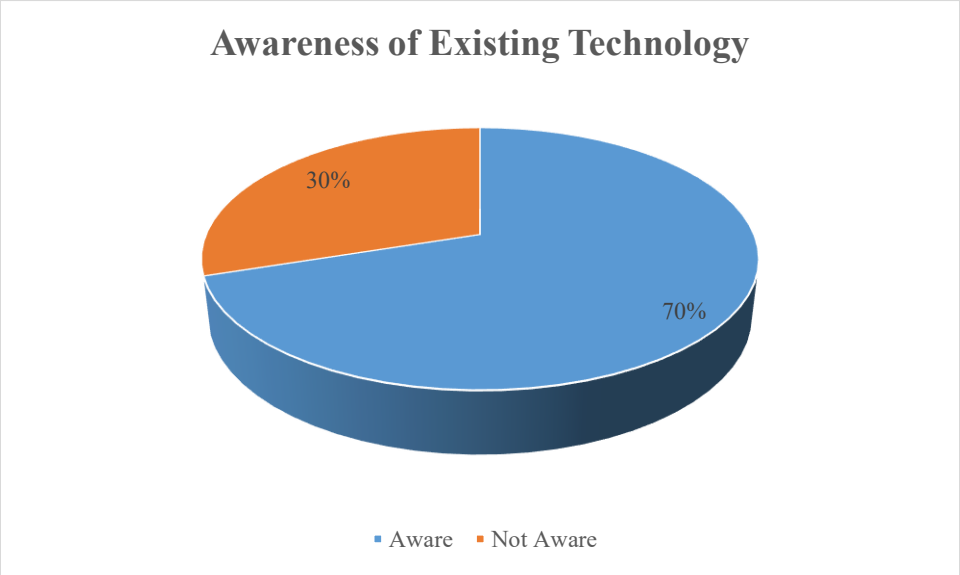

Figure 4.10: Awareness of Existing Solutions

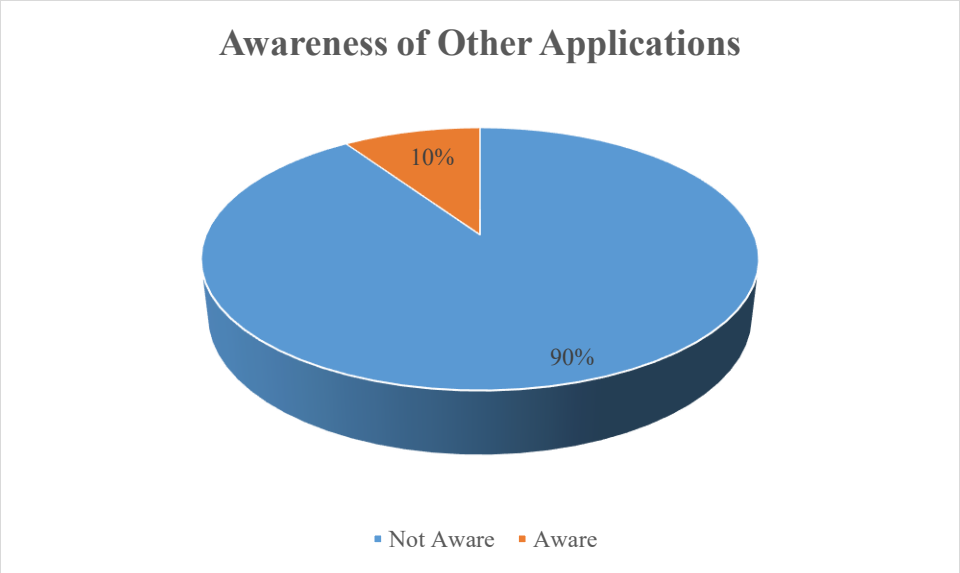

Figure 4.11: Awareness of Other Applications

4.2.10 Response to Proposed Solution

The respondents mentioned some of the features used to administer access control on mobile devices. Out of the 42 respondents who were aware of existing technologies that provide

access control features, all of them stated that the most common method used was using a password on a list of blocked applications. All the respondents were further given suggestions to the proposed solution where they were to give feedback on the acceptability of the proposed solution. The proposed solution was to be an application launcher which can create user profiles and block applications uniquely for each profile. The blocked applications and settings will not be visible on the application launcher. 80% of the respondents strongly agreed to use the proposed solution, 15% of the respondents just agreed, only 5% neither agreed nor disagreed and no respondent disagreed or strongly disagreed. Figure 4.12 shows a summary of the respondent's response.

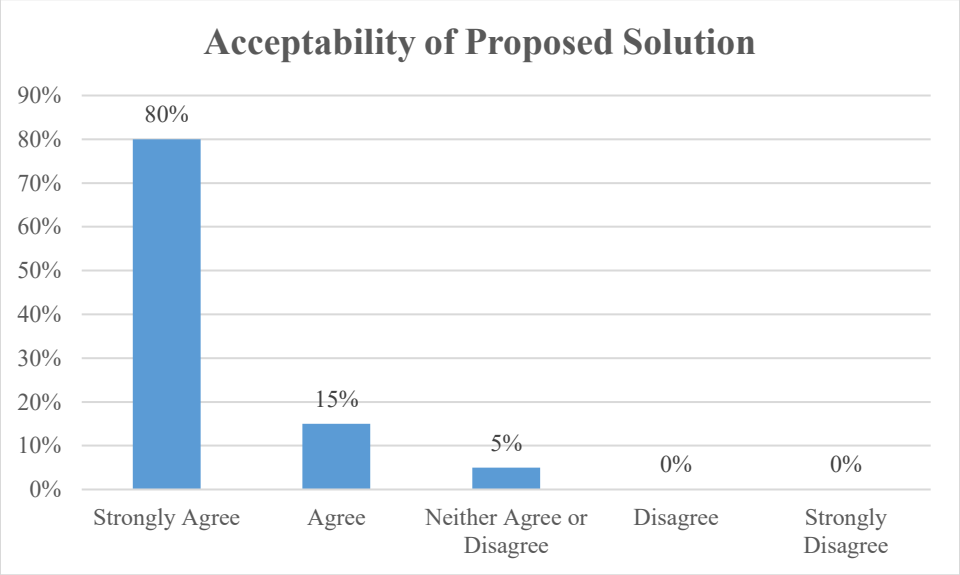

Figure 4.12 : Acceptability of Proposed Solution

4.2.11 Conclusions

Based on the analysis of the data provided by the respondents, the results led to the following conclusions that will aid in the design of the proposed system:

i. The Android platform was the preferred platform for developing the proposed system.
ii. There were challenges faced by respondents to secure their phones since threats ranged from people they know to unknown individuals in scenarios such as phone theft. A solution needed to be designed to mitigate threats from all parties.
iii. The application should only display what the phone owner wants to be visible on the phone based on the user profiles created by the phone owner.

iv. The proposed solution would be accepted by majority of the users.

4.3 System Architecture

System architecture is a clarification of parts that make up a system, the behavioural details of those parts, mechanisms and patterns, which collaborate with each other as shown in Figure 4.13.

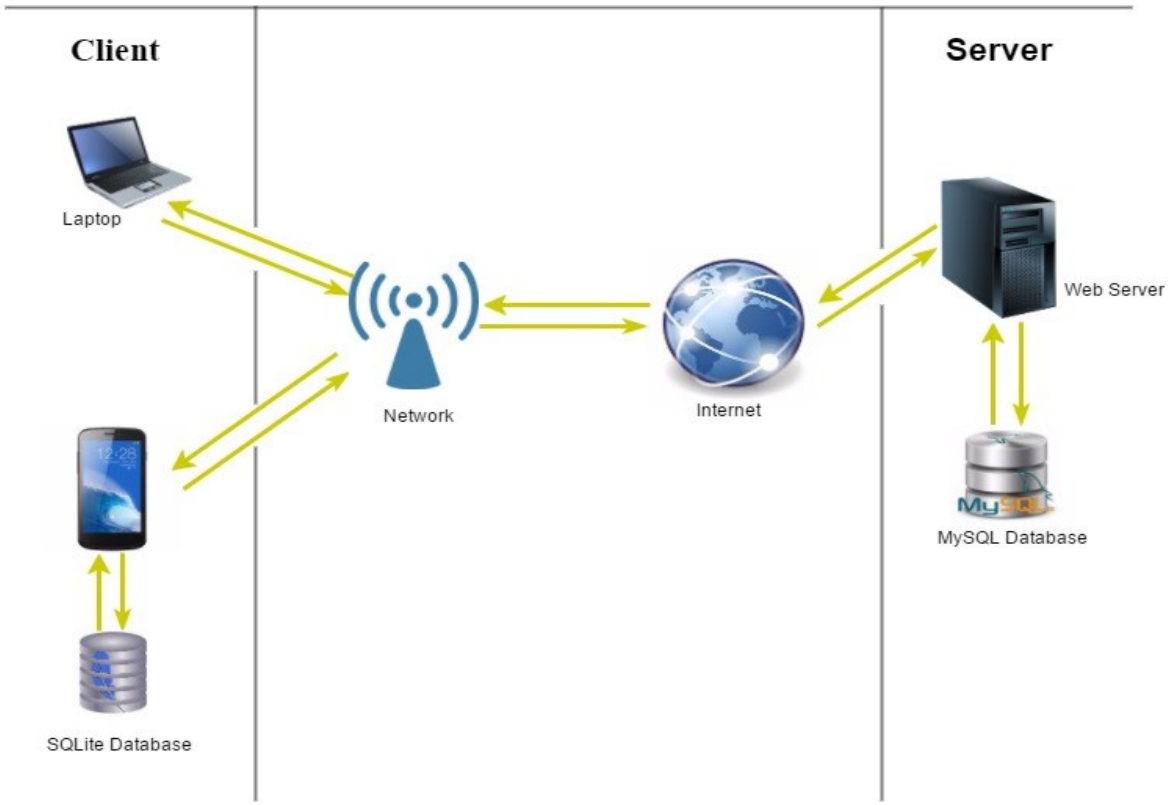

Figure 4.13: System Architecture

4.3.1 Explanation of the Architecture

The Client-Server architecture was the architecture adopted for the development of the system. The client side consisted of the Android mobile application and the backend portal for administration purposes. The mobile application will require the owner of the phone to first register before using the mobile application. Through a network connection, the owner of the phone will send registration details using a POST method to the remote server and the details stored in a MySQL database. The main reasons for using POST method to make requests to the server is to ensure security of the user details and to also transmit more data in one request.

The mobile application makes use of the mobile phone's SQLite database to manage user profiles and to maintain a record of the blocked applications for each user profile. The application launcher will constantly check the SQLite database to determine the current and settings therefore ensuring only the most allowed applications are displayed on the application launcher. The records of blocked applications and settings are sent to the remote database server which will be used by the administrator to carry out data analysis and generating reports. Tableau was the software used to analyse data stored in the remote database.

The web server is where the PHP scrips reside and they are responsible for the logic on the backend, handling requests from clients, responding to these requests and interaction with the MySQL database.

4.4 System Design

This section will focus on the design structure which fulfils the functional, non-functional requirements and research objectives. This involves the use of diagrams to logically represent the solution and to give insight on the actual implementation of the system. The design components used were:

i. Use Case Diagrams
ii. Sequence Diagrams
iii. Class Diagrams
iv. Entity Relationship Diagrams
v. Database Schema
vi. User Interface Flow Diagrams

4.4.1 Use Case Diagrams

Use Case Diagrams are behavioural diagrams used to show the functionalities of a system and how different users known as actors, interact with the system so as to achieve a certain goal. The following are the actors who interact with the system:

Phone Owner- This includes the actual owner of the phone and is responsible for managing all aspects of the application. The Phone owner is responsible for creating guest accounts, blocking applications and managing these accounts and settings.

Guest – These include any person who does not own the phone and is given credentials by the phone owner in accessing a guest account. The guest can only view and use allowed applications.

System Administrator – These include the software developers who are responsible for the management and maintenance of the system and also manage the users (phone owners).

The following are the main processes in this system.

Register- The primary actor of this process is the phone owner who intends to administer access control features.

Login and Logout- The primary actors are the phone owner, system administrator and the guest. This is required to access different modules of the system.

Manage User Profiles- The primary actor is the phone owner who intends to create profiles for guest users, and further update or delete the profiles. Each profile will have a unique password assigned to it that will be used by guest users to access the launcher application.

Block Applications and Settings- The primary actor is the phone owner who blocks applications uniquely for each profile.

Search Applications- The primary actors are the phone owner and the guest where the phone owner may do a search with an aim of using the application, blocking the application or unblocking the application and the guest will perform a search with an aim of easily identifying the application and proceed to using it.

Manage Users- The primary actor is the system administrator where monitoring user activity and deletion of users can be executed.

Generate Report- The primary actor is the system administrator who makes use of analytical software to generate reports that will aid in better decision making.

Figure 4.14 shows how these users interact with the system.

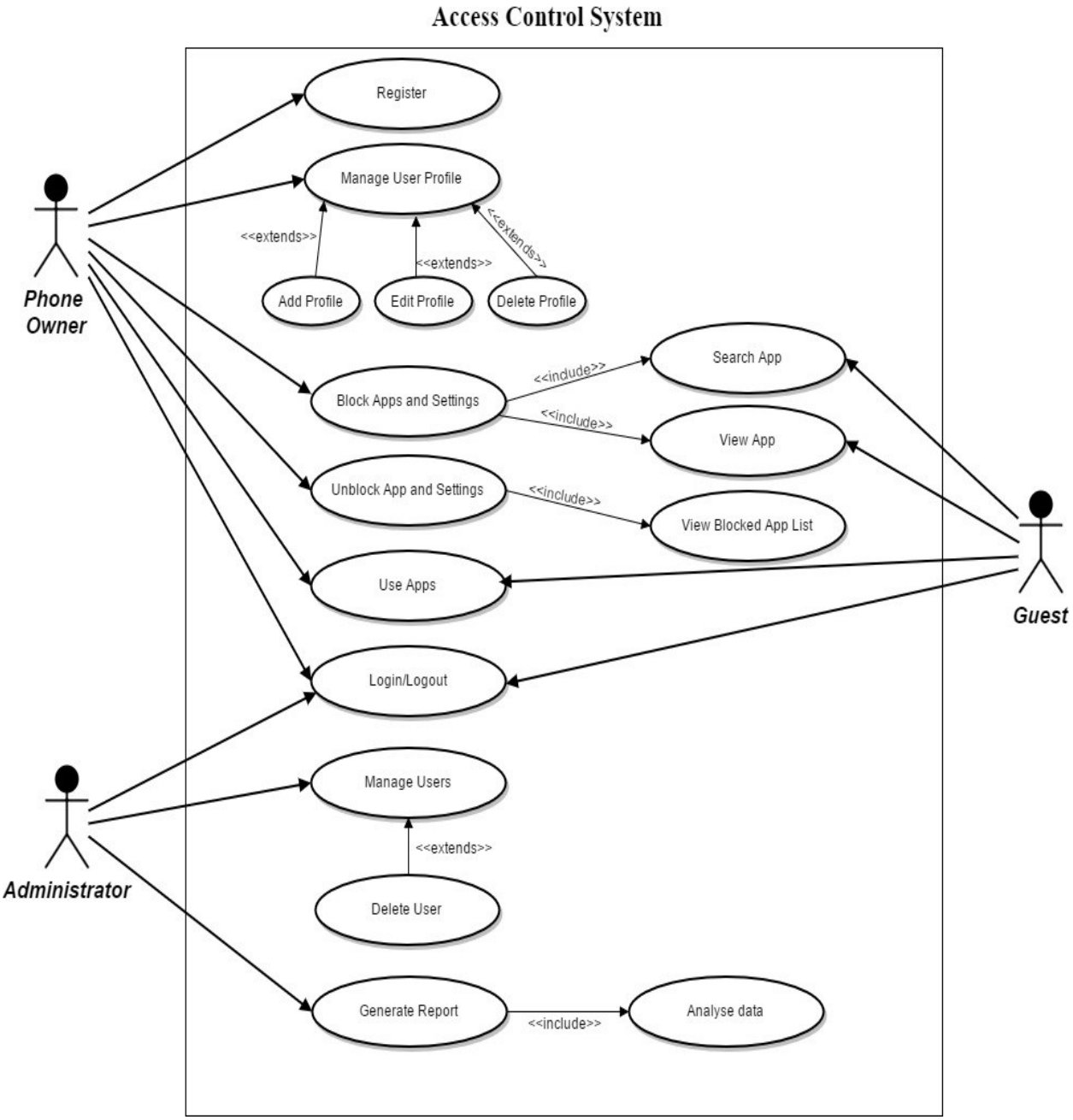

Figure 4.14: Use Case Diagram

4.4.2 Use Case Description

4.4.2.1 Use Case 1: Register

Table 4.2: Register Use Case Description

Use Case Name:	**Register**

Scenario:	Involves the phone owner	
Event(Trigger):	Phone owner sends registration request.	
Brief Description:	Phone owner provides personal information on and a password. System saves this information.	
Actors:	Phone Owner	
Stakeholders:	System Administrator, Phone Owner	
Preconditions:	Phone owner must provide accurate personal information.	
Post conditions:	New account object created. Unique Id generated to uniquely identify phone owner. Id to be saved in SQLite database during Login Process.	
Flow of events	Actor 1. Phone owner enters personal details into the system.	System 1.1 Saves personal details and generate unique ID.

4.4.2.2 Use Case 2: Login/Logout

Table 4.3: Login/Logout Use Case Description

Use Case Name:	**Login/Logout**	
Scenario:	The actors intend to access or exit the application or system. Involves the phone owner, guest and system administrator.	
Event(Trigger):	Actors click on the sign in or sign out button.	
Brief Description:	The actors enter their credentials and trigger the login process when intending to login but click on the sign out button when intending to logout which triggers the logout process.	
Actors:	Phone Owner, Guest, System Administrator	
Stakeholders:	Phone Owner, System Administrator.	
Preconditions:	For the Login process, the actor must be a registered and account must be active. For the logout process, the actor must have logged in to the system.	
Post conditions:	For Login process, successful authentication will direct the user to the home screen while unsuccessful authentication will generate a message that prompts the user to enter the correct details. For the Logout process, the user will be directed to the login screen.	
Flow of events	Actors	System

	1. Enter username and password, then press login button. 2. Perform tasks when login process is successful 3. Logout by pressing the sign out button	1.1Checks if the username and passwords match with the details in the database. 1.2 Sends response to user. 1.3 Creates a session 3.1 Terminates the session and redirects to login screen.

4.4.2.3 Use Case 3: Manage User Profile

Table 4.4: Manage User Profiles Use Case Description

Use Case Name:	**Manage User Profile**
Scenario:	The phone owner intends create, update and delete user profiles depending on his/her preference. Involves the phone owner and guest.

Event(Trigger):	Need for a new profile, need for updating a profile or need for removing a profile.	
Brief Description:	The phone owner creates a new profile, updates or deletes a guest profile.	
Actors:	Phone Owner	
Stakeholders:	Guest	
Preconditions:	The phone owner must be a registered user. When creating a new profile, the profile name must not be existing. A profile must be existing in order to perform updates or delete operations on a profile.	
Post conditions:	A newly created profile with a new list of applications that provide an option for blocking. An updated profile with altered details and settings. The deleted profile will be removed from the list of user profiles and all its settings and details removed from the SQLite database.	
Flow of events	Actors 1.Enter profile name and password/pin	System 1.1 Sends information to SQLite database. 1.2 Creates new user profile

	2. Select a profile and edit details. 3. Select profile and select the delete operation.	2.1 Sends details to database and returns response to user. 3.1 Runs a delete query on the database and removes all the details of the user profile.

4.4.2.4 Use Case 4: Block Applications and Settings

Table 4.5: Block Application and Settings Use Case Description

Use Case Name:	**Block Applications and Settings**
Scenario:	The phone owner intends to block certain applications and settings so that they are not accessible to other individuals.
Event(Trigger):	Hiding applications and settings.
Brief Description:	The phone owner will create a user profile and select the applications and settings he/she intends to block from other users.
Actors:	Phone Owner

Stakeholders:	Guest, System Administrator.	
Preconditions:	Phone owner must have a registered account. A user profile must be created or must exist.	
Post conditions:	Applications and settings will be hidden from the guest user. The SQLite database will be updated with the current data. The details will be sent to the remote database for analysis.	
Flow of events	Actors 1. Select user profile 2. Select settings and applications to block. 3. Logout and view launcher application.	System 1.1 Retrieves ID from the user profile table 2.1 Updates records based on the retrieved ID 2.2 Updates the launcher application hiding the blocked apps and settings.

4.4.2.5 Use Case 5: Search Application

Table 4.6: Search Application Use Case Description

Use Case Name:	**Search Application**	
Scenario:	The phone owner and guest intend to easily look for an application using its package name.	
Event(Trigger):	Look for an application in the fastest way possible.	
Brief Description:	The phone owner and guest will search for an application when the list of applications are many and it becomes tiresome to look for the application sequentially.	
Actors:	Phone Owner, Guest	
Stakeholders:	Phone Owner, Guest	
Preconditions:	Phone owner and guest must have a registered account and user profile respectively. Application to be searched must be installed.	
Post conditions:	Searched application only appears on the list view or application launcher.	
Flow of events	Actors 1. Enter application package name	System 1.1 Performs like searches as every character is input one at a time.

	2. View searched application	1.2 Displays results on launcher or list view.

4.4.2.6 Use Case 6: Manage Users

Table 4.7: Manage Users Use Case Description

Use Case Name:	**Manage Users**
Scenario:	The system administrator monitors the activity of the phone owners and can delete their accounts in case of inactivity or violation of policy.
Event(Trigger):	Need for monitoring user activities.
Brief Description:	The system administrator monitors the activity of the phone owners and can delete their accounts.
Actors:	System Administrator
Stakeholders:	Phone Owner
Preconditions:	Phone owner must have a registered account. The phone owner must create guest profile accounts.

Post conditions:	Deleted Account. Analysis of user actions.	
Flow of events	Actors 1. Select user 2. Monitor activity 3. Delete user if inactive depending on policy.	System 1.1 Retrieves ID from the users table and all records associated with the user. 3.1 Removes basic data from database but leaves data for analytics and report purposes.

4.4.2.7 Use Case 7: Generate Report

Table 4.8: Generate Report Use Case Description

Use Case Name:	**Generate Report**
Scenario:	The system administrator analyses data from many phone owners and generates reports.
Event(Trigger):	Need for reports to aid in decision making.
Brief Description:	The system administrator generates reports after analysing data.

Actors:	System Administrator	
Stakeholders:	Phone Owner	
Preconditions:	Administrator must login to the system.	
Post conditions:	Analysis showing different presentation of the data collected from phone owners Intelligent reports.	
Flow of events	Actors 1. Send report request. 2. Views Report	System 1.1 Analyses data stored in database and generates reports. 1.2 Sends results with different representation of the analysed data.

4.4.3 Sequence Diagrams

A Sequence diagram is used to show the sequence of steps that different users of the system take to complete a task. The interaction between different entities are clearly outlined, in this case five system entities were used to demonstrate how users interact with the system and the different

messages and responses sent during the interactions. Figure 4.15 shows the sequence diagram for this system.

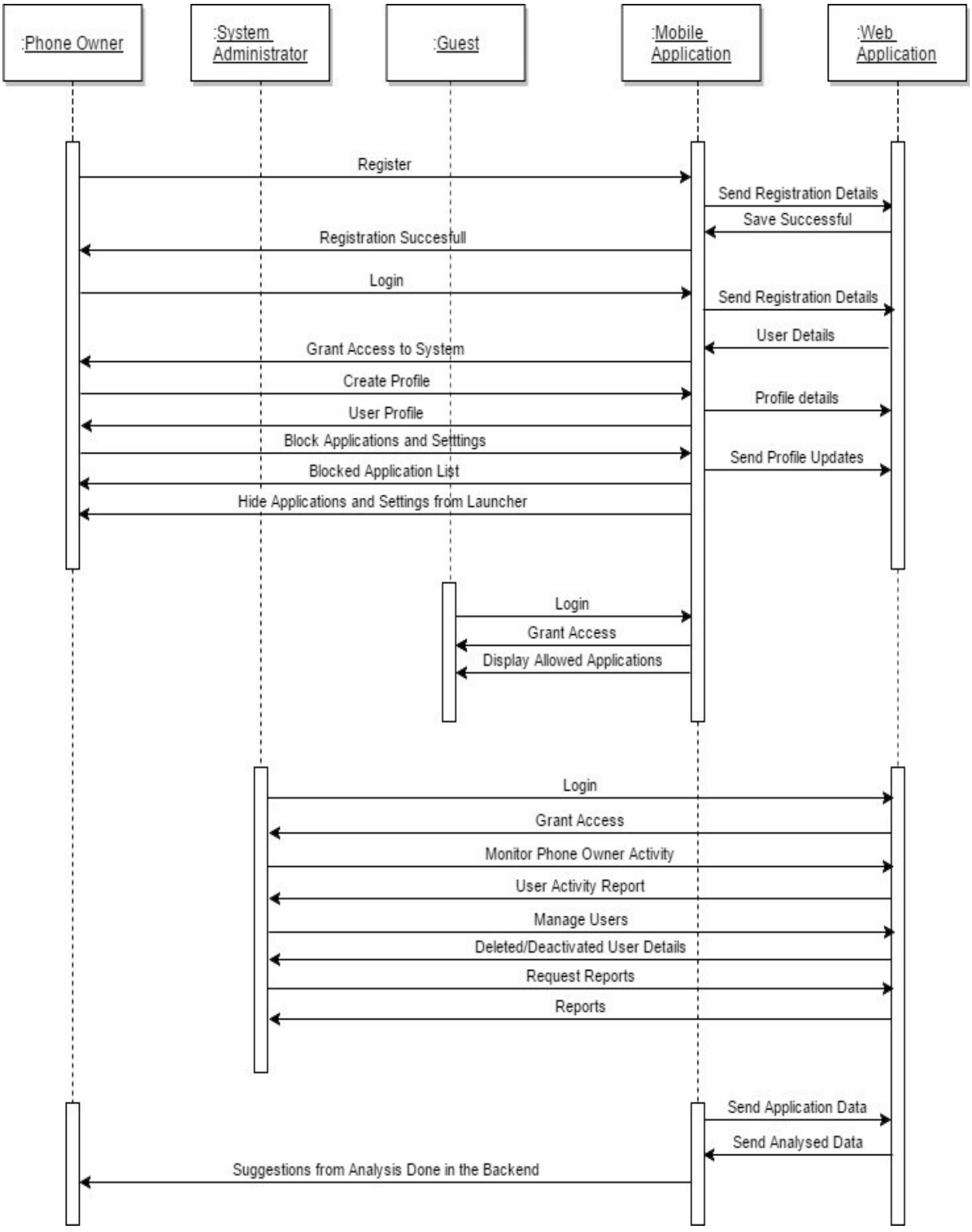

Figure 4.15: Sequence Diagram

4.4.4 Class Diagram

A class diagram is used to show the relationships between object and classes in a system. It further shows the attributes of an object or a class and the methods contained in that class. Figure 4.16 shows the class diagram for this system.

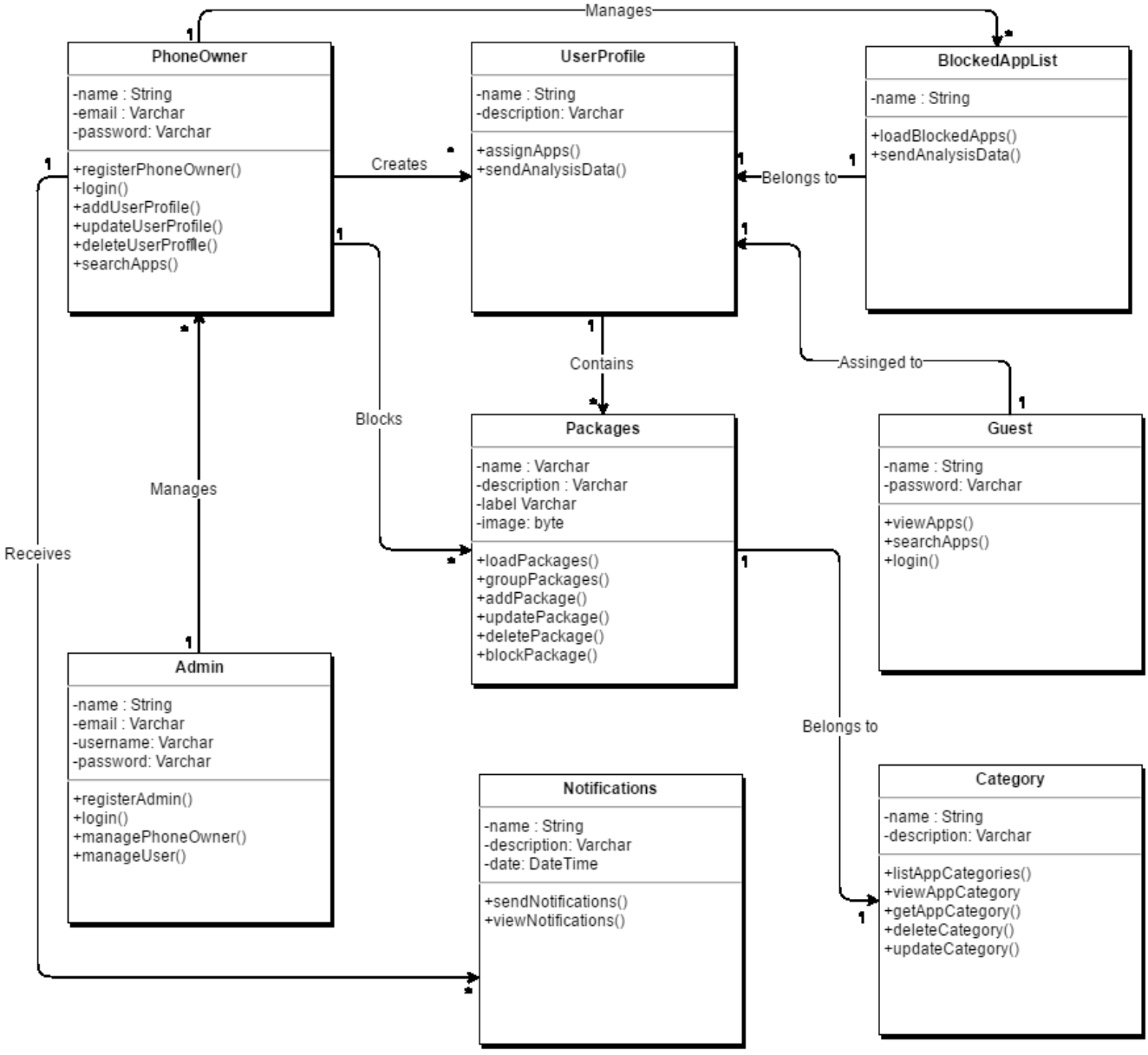

Figure 4.16: Class Diagram

4.4.5 Database Schema

Database Schemas represent the logical view of an entire database. Entity Relationship Diagrams are part of the database schema which are commonly used to show the relationship

between different entities of a system. Figure 4.17 and 4.18 show the ERD diagrams for the proposed system with a tabular description.

4.4.5.1 ERD for Offline (SQLite) Database

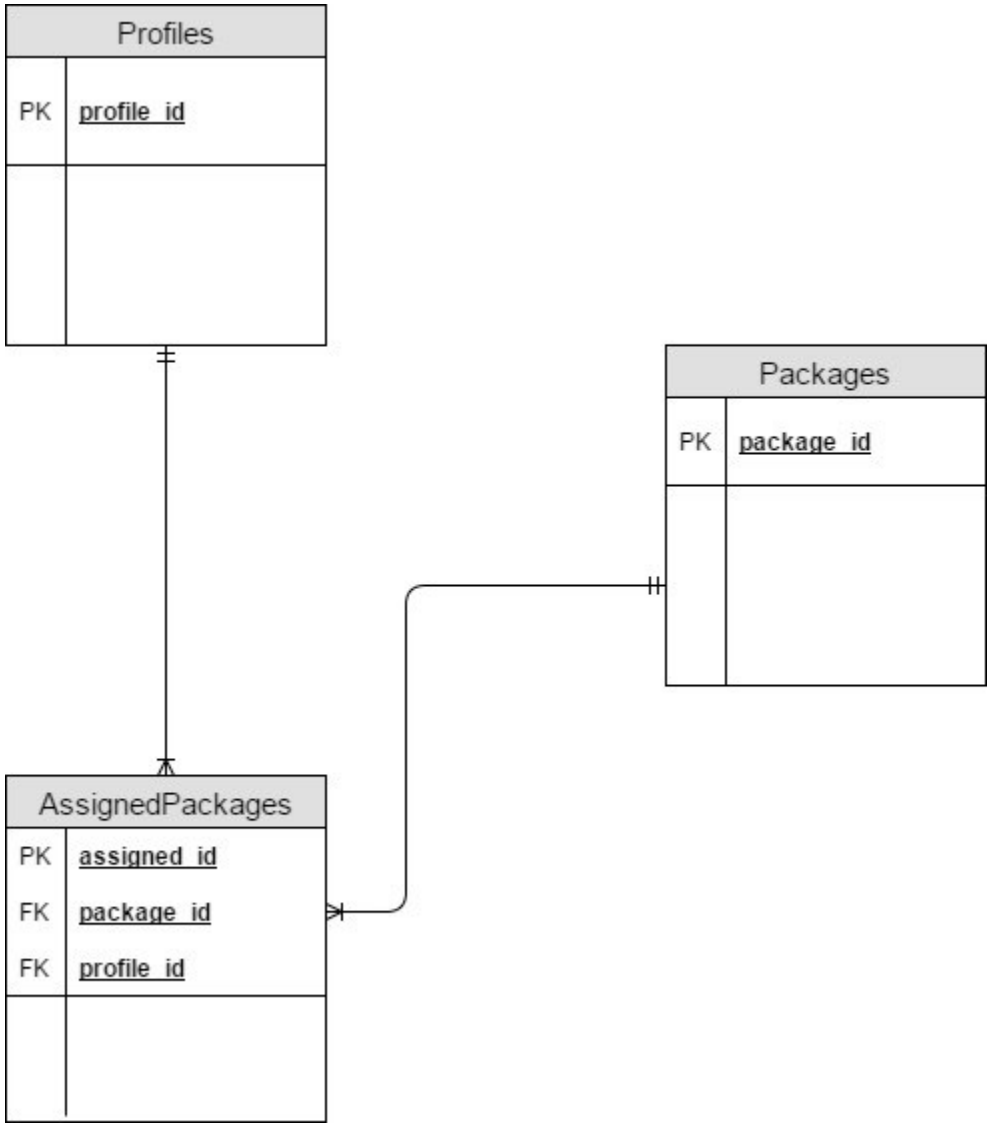

Figure 4.17: ERD for Offline Database

4.4.5.1.1 ERD Description

Figure 4.17 above shows the relationship between the entities of the offline database. The packages entity has a mandatory one to many relationship with the assigned packages entity and the assigned packages has a mandatory one relationship with the packages entity. This means that there could be multiple instances of a package associated with the assigned packages entity. A

mandatory one to many relationship also exist between the profile entity and the assigned packages entity. This ensures that an application is blocked based on a profile. Multiple instances of a profile and a package can be associated with the assigned packages entity. This means that a single package can be blocked based on all the profiles that exist.

4.4.5.1.2 Description of Entities

The offline database contains three entities which include Profiles, Packages and Assigned Packages. The following section explains each entity in detail.

Profiles- This entity will hold data for user profiles which are added by a user. The Profiles entity will hold data for the profile name, the pin, the date which will capture the date the profile was added and profile id which will be the primary key that uniquely identifies a record in the Profiles entity. The pin will be used by the system to determine which profile will be loaded.

Packages- This entity will hold data for all the applications that are installed on the phone. The package id attribute will uniquely identify each package therefore it will be the primary key of the packages entity. The package name attribute will hold data for the name of the application and the date attribute will be used to capture the date when the application was added in the database.

Assigned packages- This entity will hold data for the applications that have been assigned to a specific profile. The assigned id will be the primary key which uniquely identifies a record in the table. The package id will be a foreign key which is a primary key to the packages table. This attribute will enable an application to be assigned to a specific profile where the profile will be specified in the profile id attribute which is a foreign key to the profiles table. The status attribute will hold data that will determine whether the assigned application will be displayed or blocked. The date attribute will be used to capture the date in which the application was assigned to a specific profile.

The entities discussed above can be summarised in tables as shown in Table 4.9, 4.10 and 4.11 below.

Profiles Table

Table 4.9: Profiles Table

Column Name	**Data Type**	**Index**
profile_id	Int(30)	Primary Key
name	Varchar(255)	
pin	Varchar(20)	
date	Datetime	

Packages Table

Table 4.10: Packages Table

Column Name	**Data Type**	**Index**
package_id	Bigint	Primary Key
package_name	Varchar(100)	
date	Datetime	

Assigned Packages Table

Table 4.11: Assigned Packages Table

Column Name	**Data Type**	**Index**
assigned_id	Bigint	Primary Key
package_id	Int(30)	Foreign Key
profile_id	Int(30)	Foreign Key
status	Varchar(100)	
date	Datetime	

4.4.5.2 Online (Hosted) Database

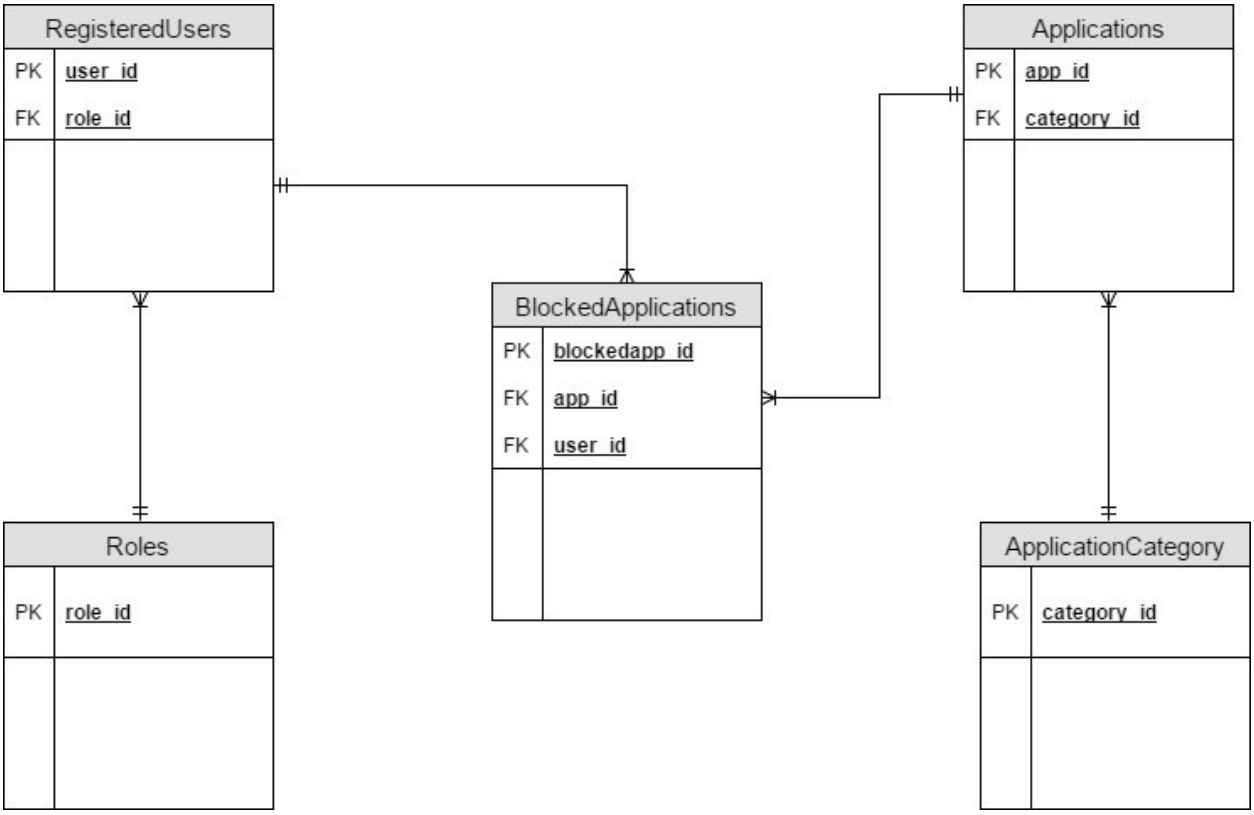

Figure 4.18: Entity Relationship Diagram for Hosted Database

4.4.5.2.1 ERD Description

Figure 4.18 above shows the relationship between the entities of the online database. The roles entity has a mandatory one to many relationship with the registered users entity and the registered users entity has a mandatory one relationship with the roles entity. This means that a registered user needs to be associated with only one role but there can be multiple instances of a role associated with the registered user relationship. There exist a one to many relationship between the registered users entity and the blocked applications entity since there can be multiple instances of a registered user associated with the blocked applications entity. This means that the registered user can block multiple applications. The application entity has a one to many relationship with the blocked applications entity since multiple instances of a single application can be associated with the relationship with the blocked applications entity. This means that a single application can be blocked by many registered users.

4.4.5.2.2 Description of Entities

The online database contains five entities which include Registered Users, Roles, Applications, Application Category and Blocked Applications. The following section explains each entity in detail.

Registered Users- This entity will hold data for users who have registered with the application or have system users who have been added by a system administrator. The user id attribute will be the primary key which uniquely identifies each user in the table. The name and email attributes will hold the user's name and email respectively. The role id attribute will be a foreign key but primary key in the roles table. This attribute will hold the value that will determine the role of the user. The encrypted password attribute will hold the password for the user which will be used during user authentication. The date attribute will capture the date the user was registered.

Roles- This entity will hold data for all the roles defined in the application. The roles will further be assigned to a registered user. The role id attribute will hold data that will uniquely identify each role in the roles table. The name attribute will be used to hold that for the role name and the date attribute will be used to capture the date when the role will be added.

Application Category- This entity will hold data for all the categories of applications that exist in the registered user's phones. The category id attribute will hold data that will uniquely identify a record in the application category table. The name attribute will hold data for the category name of an application and the date attribute will be used to capture the date when the category will be added in the table.

Applications - This entity will hold data for all the applications that all the registered users have installed on their phone. The "app id" attribute will be the primary key which will uniquely identify a record in this table. The "app name" attribute will hold data for the name of the application and the category id attribute which is a foreign key to the application category table, will hold data which will identify the category of the application. The date attribute will be used to capture the date when the record will be added in the table.

Blocked Applications- This entity will hold data for all the applications that have been blocked by a registered user. The blocked id attribute will be the primary key which uniquely identifies a record in the table. The "app id" attribute will be a foreign key which is a primary key to the

applications table. This attribute will hold data for a blocked application based on the specified registered user who will be identified by the data that will be held by the user id attribute. The user id attribute will be a foreign key to the registered users table specifies the registered user who has installed a specific application on their phone. The date attribute will be used to capture the date when the record will be added in the table.

The entities discussed above can be summarised in tables as shown in Table 4.12, 4.13, 4.14, 4.15 and 4.16 below.

Registered Users Table

Table 4.12: Online Registered Users Table

Column Name	**Data Type**	**Index**
user_id	Int(30)	Primary key
name	Varchar(100)	
email	Varchar(100)	Unique
unique_id	Varchar(255)	Unique
role_id	Int(30)	Foreign Key
encrypted_password	Varchar(20)	
created_date	Datetime	

Roles Table

Table 4.13: Roles Table

Column Name	**Data Type**	**Index**
role_id	Int(30)	Primary Key
name	Varchar(100)	

description	Varchar(255)	
date	Datetime	

Application Category Table

Table 4.14: Application Category Table

Column Name	**Data Type**	**Index**
category_id	Int(30)	Primary Key
name	Varchar(255)	
date	Datetime	

Applications Table

Table 4.15: Applications Table

Column Name	**Data Type**	**Index**
app_id	Bigint	Primary Key
app _name	Varchar(100)	
category_id	Varchar(100)	
date	Datetime	

Blocked Applications Table

Table 4.16: Blocked Applications Table

Column Name	**Data Type**	**Index**
blocked_id	Bigint	Primary Key
app_id	Int(30)	Foreign Key

user_id	Int(30)	Foreign Key
date	Datetime	

4.4.6 User Interface Flow Diagram

The proposed solution shall consist of a mobile application and a backend for administration purposes. The phone owners and guests will use the mobile application while the backend will be used by system administrators for analysis and generating reports.

4.4.6.1 Mobile Application

Figure 4.19 shows the registration screen where the phone owner will have to register before making use of the application. After successful registration, the phone owner can login using the screen shown in Figure 4.20.

Figure 4.19: Register Phone Owner

Figure 4.20: Login as Phone Owner

Figure 4.21 shows the home screen which displays after the login process is successful. The phone owner can either select the user profiles option or the reports option from the list. When the user profiles option is selected, the user profiles screen will display as shown in Figure 4.22.

Figure 4.21: Home Screen

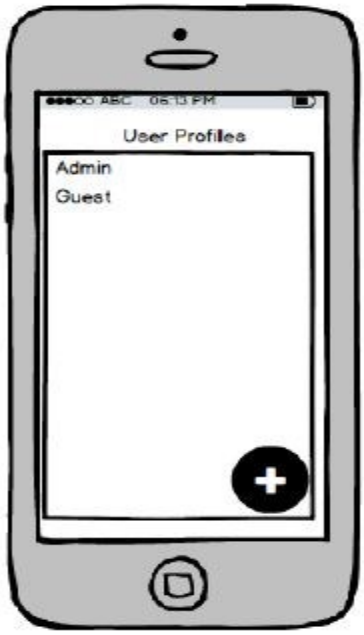

Figure 4.22: User Profiles Screen

The phone owner can add a new profile by selecting the floating button that contains a plus sign. The phone owner can also edit settings of an existing profile by selecting the desired profile in the list of options. When the phone owner selects the floating button, the “add new profile” screen will

display as shown in Figure 4.23. Alternatively, when a user profile is selected from the “User Profiles” screen, the “Profile Settings” screen will be displayed as shown in Figure 4.24.

Figure 4.23: Add New Profile Screen

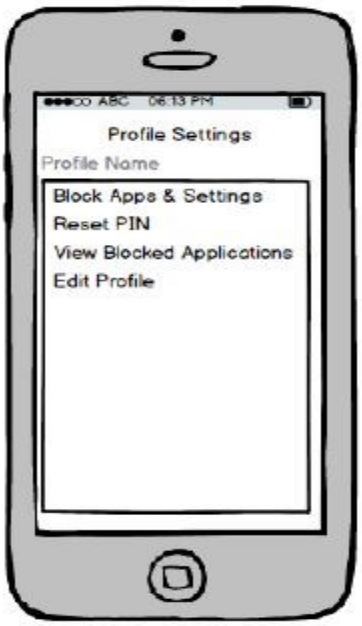

Figure 4.24: Profile Settings Screen

The phone owner can further select the “Block App & Settings” options to block applications and settings. The window “Block Applications” screen will be displayed as shown in Figure 4.25.

Figure 4.25: Block Applications Screen

When the “Reset PIN” option is selected in Figure 4.24, the screen shown in Figure 4.26 will be displayed which will ensure that the phone owner changes the PIN to be used for a specific profile.

Figure 4.26: Reset PIN Screen

When the phone user selects the “View Blocked Applications” option in Figure 4.24, the screen shown in Figure 4.27 will be displayed which will list all the blocked applications and the phone owner can open any of the applications on the list.

Figure 4.27: Blocked Application List

In order for the phone user to edit a profile, the “Edit Profile” option in Figure 4.24 will lead to the screen shown in Figure 4.28 that will provide these functionality.

Figure 4.28: Edit Profile Screen

If the phone owner intends to view reports, the “View Report” option in the home screen as shown in Figure 4.21 can be selected. This action will lead to the “Report Screen” being displayed as shown in Figure 4.29.

Figure 4.29: Report Screen

In order for a different user to access the launcher application, he/she will have to input the PIN issued by the phone owner. This PIN will determine the profile that will be loaded as a result determining the applications to be displayed on the launcher. Figure 4.30 shows the screen used to input the PIN. After successful authentication, the launcher will be displayed as shown in Figure 4.31.

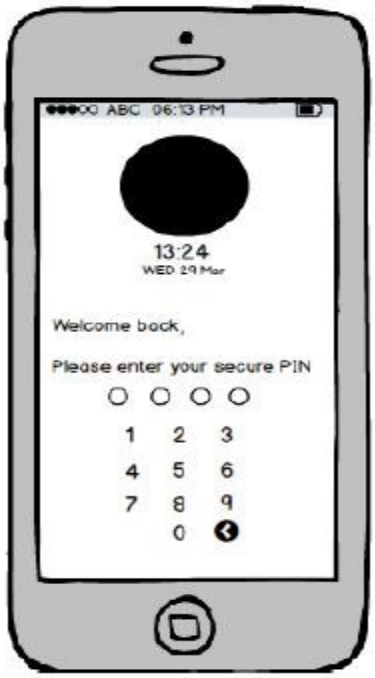

Figure 4.30: Launcher Authentication Screen

Figure 4.31: Launcher Screen

4.4.6.2 Web Application

The system administrator will handle management activities through a web portal which will require authentication as shown in Figure 4.32. Successful authentication will display the web portal as show in Figure 4.33.

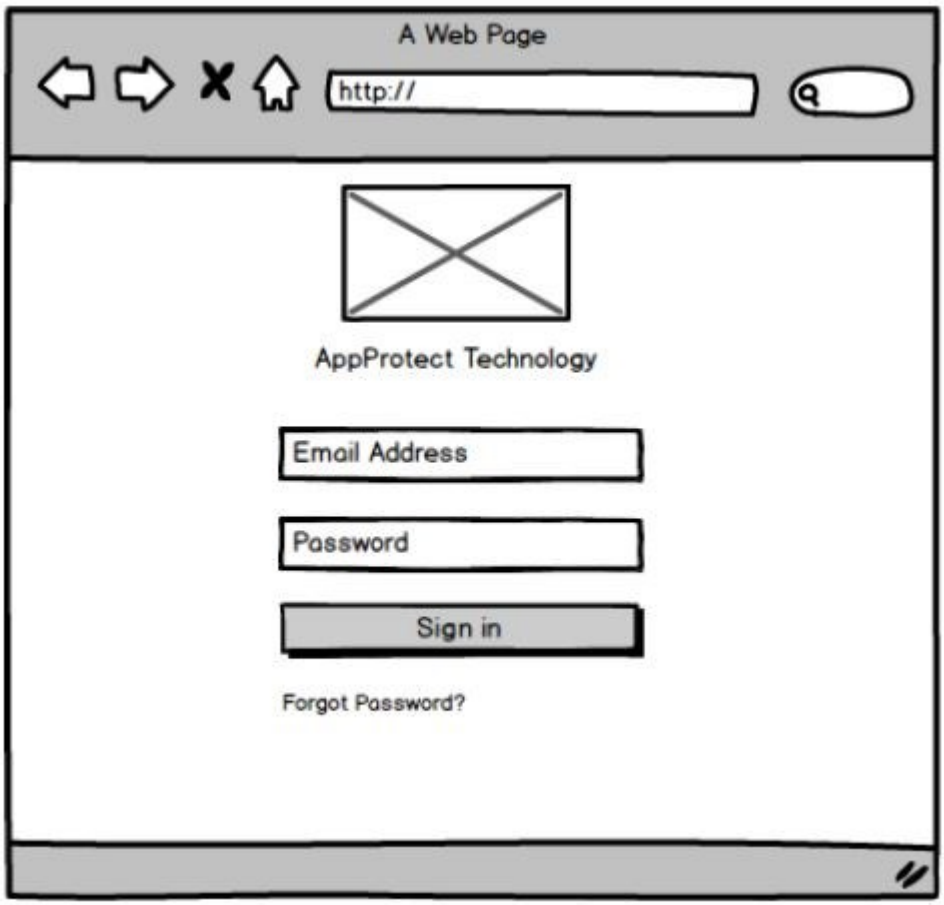

Figure 4.32: Backend Login Window

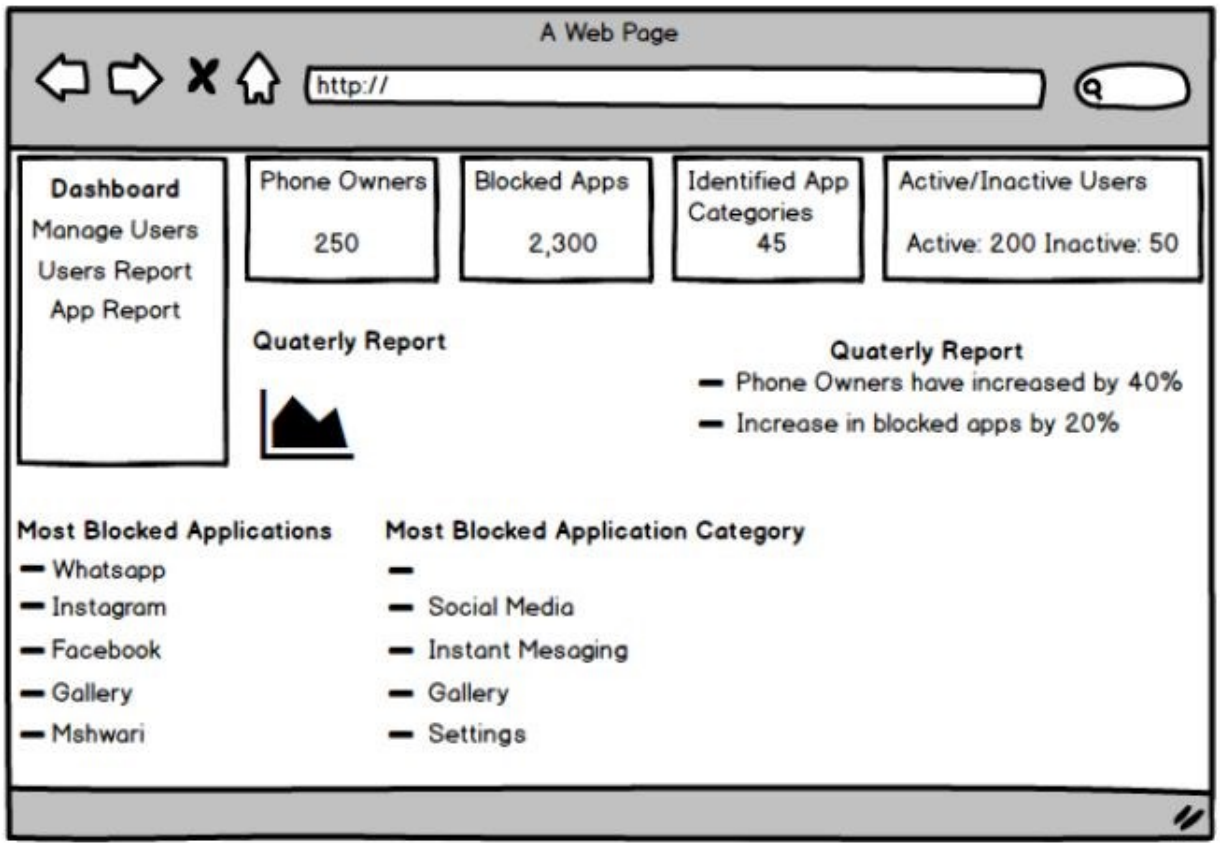

Figure 4.33: Web Portal Window

4.5 Conclusions

System analysis and design helped understand the user requirements and aided in designing the system according to the user's needs. Interaction diagrams such as sequence diagrams, UML notations such as class diagrams and use case diagrams and data modelling diagrams such as ERD were used to better understand the system and uniquely define the system components. The architecture to be used is a client server architecture which will be best suited to implement the proposed solution.

Chapter 5: System Implementation and Testing

5.1 Introduction

This chapter explains how the implementation and testing of the proposed system was carried out. All the major functionalities of the proposed system were implemented and tests were performed on the system. The tests have been clearly explained to help demonstrate how the application implements the functional and non-functional requirements and the objective of this research.

5.2 System Implementation

5.2.1 Home Screen

After successful authentication of login credentials, the home screen as shown in Figure 5.1 will be displayed to the phone owner. The phone owner can either navigate to user profiles, reports or settings by selecting one of the options on the home screen.

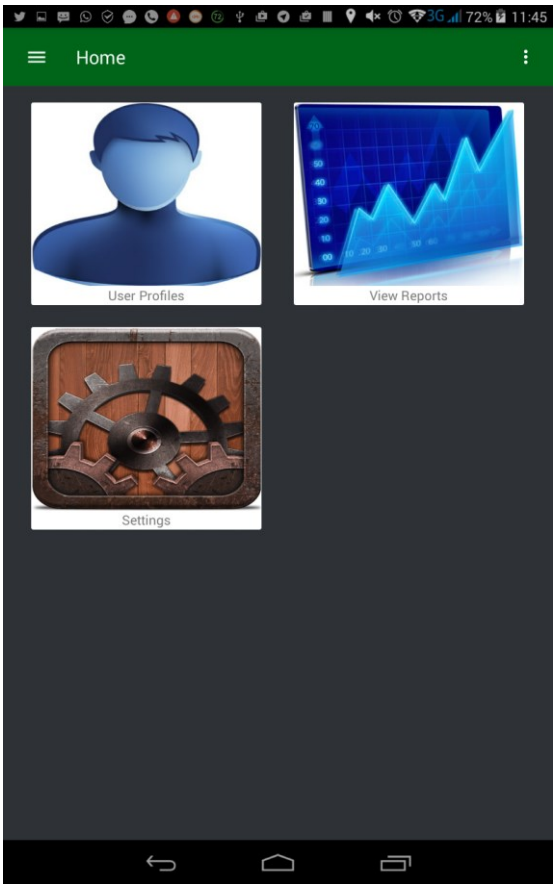

Figure 5.1: Home Screen

5.2.2 Navigation Drawer Screen

The navigation drawer contains other options and functionalities that the application supports. It ensures easy navigation to the core functionalities of the system which includes home, reports, settings, help, about and sign out options. Figure 5.2 shows the navigation drawer screen.

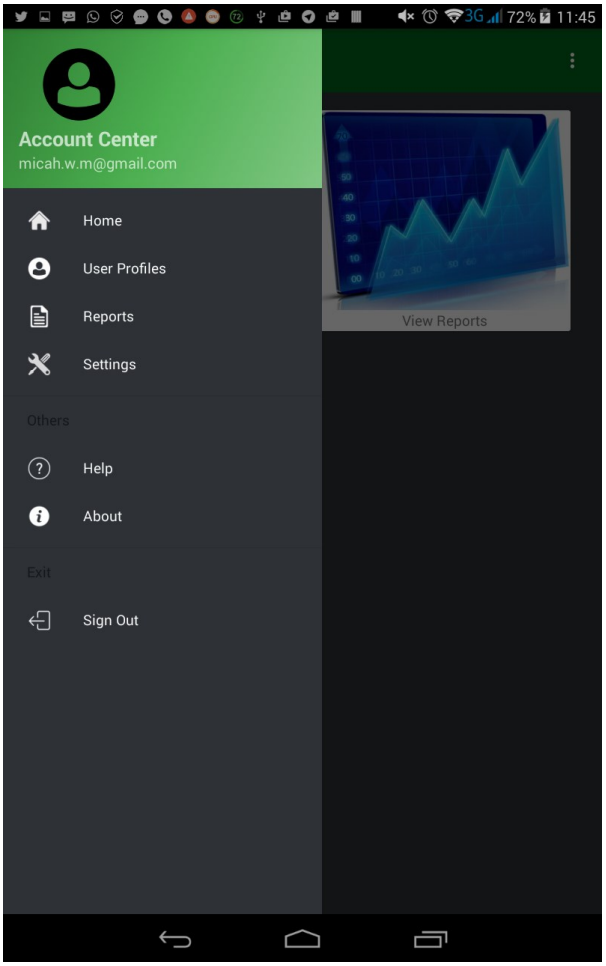

Figure 5.2: Navigation Drawer Screen

5.2.3 User Profiles Screen

This screen shows the list of user profiles that have already been added. By default, the administrator profile will exist and the phone user can further make changes to it. This screen enables the phone owner to open the “add new profile” screen by selecting the floating button that contains a plus sign. Figure 5.3 below shows the User Profiles Screen.

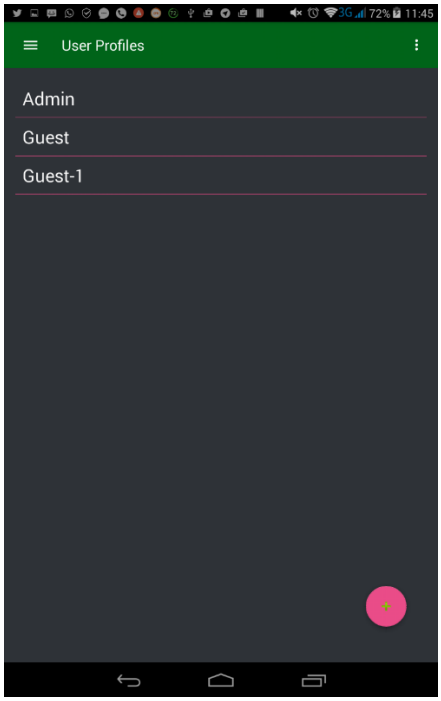

Figure 5.3: User Profile Screen

5.2.4 Add New Profile Screen

This screen enables the phone owner to add a new profile. This screen can be opened by selecting the floating button contained in the “User Profile” screen as shown in Figure 5.3. Figure 5.4 shows the “Add New Profile” screen Page.

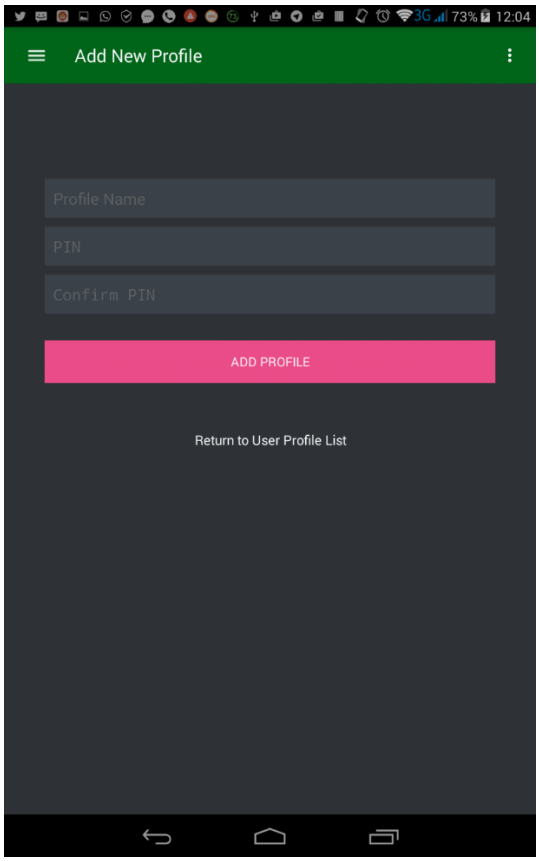

Figure 5.4: Add New Profile Screen

5.2.5 Profile Settings Screen

From the profile lists in the “User Profile” screen in Figure 5.3 the phone owner can make changes to that profile by selecting the desired profile. This will open a screen displaying a list of options that can be selected to perform further actions to the selected profile. The phone owner can either block or unblock applications, reset pin for the selected profile, view blocked applications or edit the profile name. The screen shown in Figure 5.5 shows the “Profile Settings” screen.

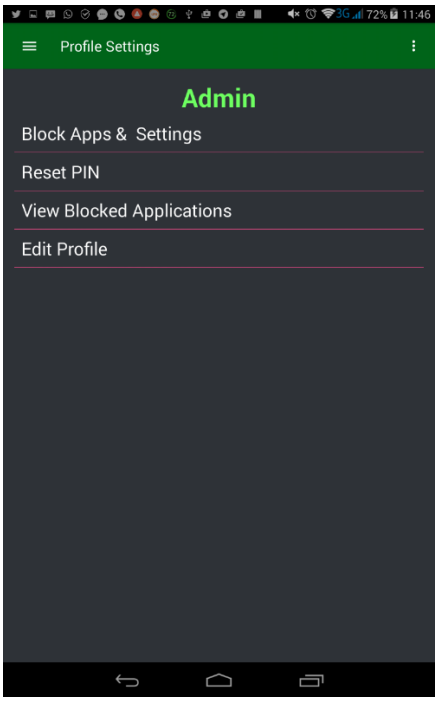

Figure 5.5: Profile Settings Screen

5.2.6 Block or Unblock Application Screen

The phone owner can access this window by selecting the “Block Apps & Settings” option in the “Profile Settings” screen shown in Figure 5.5 above. This will lead to opening the “Block / Unblock Application” screen similar to the one shown in Figure 5.6. This screen will ensure the phone owner to determine the applications that will be displayed on the application launcher when authenticating using the assigned pin.

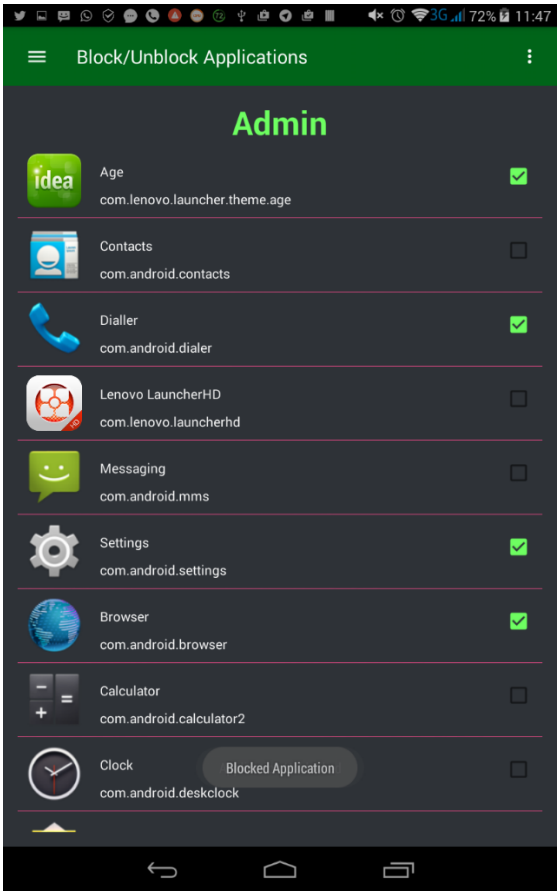

Figure 5.6: Block or Unblock Application Screen

5.2.7 Reset Pin Screen

The phone owner can access this window by selecting the “Reset PIN” option in the “Profile Settings” screen shown in Figure 5.5. This will lead to opening the “Reset PIN” screen similar to the one shown in Figure 5.7. The phone owner can therefore reset the pin for the selected profile.

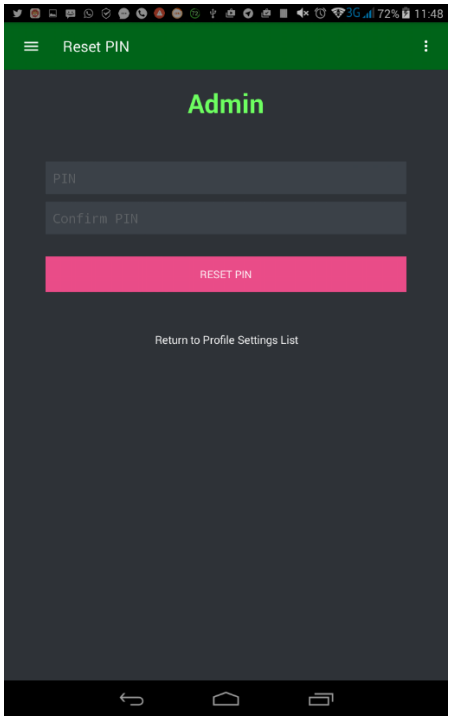

Figure 5.7: Reset Pin Screen

5.2.8 Blocked Applications Screen

The phone owner can access this window by selecting the “View Blocked Applications” option in the “Profile Settings” screen shown in Figure 5.5. This will lead to opening the “Blocked Applications” screen similar to the one shown in Figure 5.8. The phone owner can view the blocked applications for a specific profile and further open the application by selecting the desired application from the list.

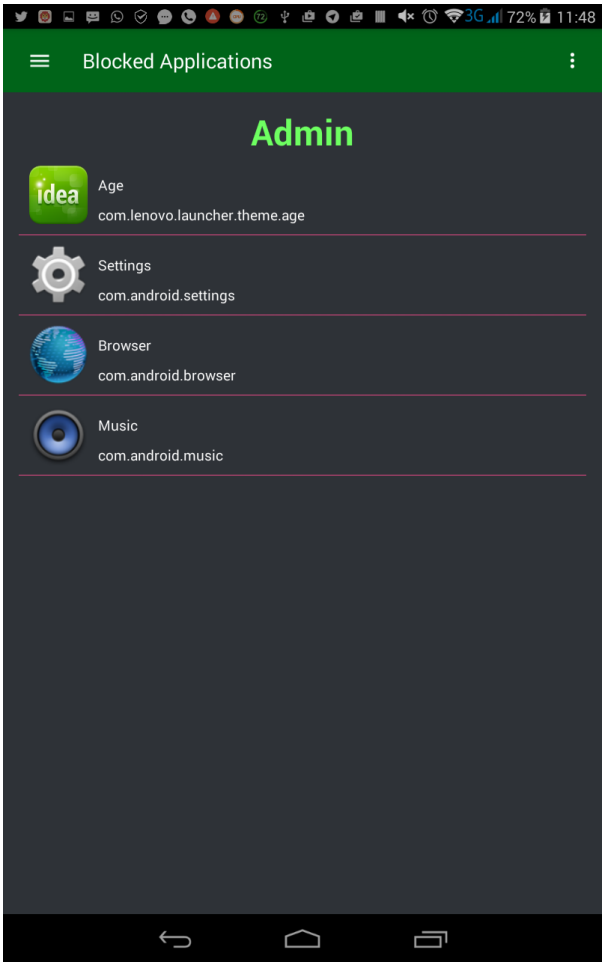

Figure 5.8: Blocked Applications Screen

5.2.9 Update Profile Screen

The phone owner can access this window by selecting the “Edit Profile” option in the “Profile Settings” screen shown in Figure 5.5. This will lead to opening the “Blocked Applications” screen similar to the one shown in Figure 5.9. The phone owner can edit the name of the selected profile

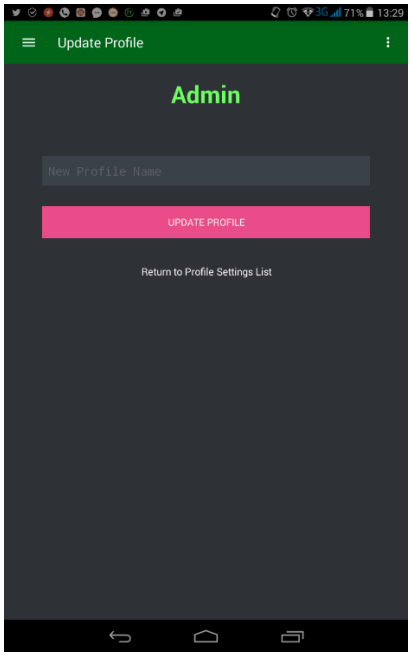

Figure 5.9: Update Profile Screen

5.2.10 Login Launcher Screen

When the phone owner finishes to setup the user profiles and signs out, the screen shown in Figure 5.10 will be displayed. This screen enables different users access the application launcher through providing the credentials given to them by the phone owner.

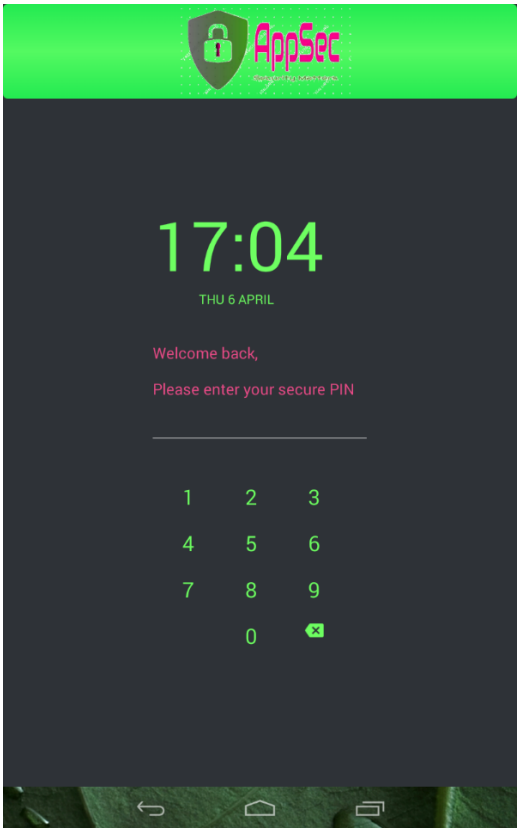

Figure 5.10: Login Launcher Screen

5.2.11 Launcher Application Screen

This is the screen demonstrating the main functionality of the system. After successful authentication in Figure 5.10 using the PIN assigned by the phone owner, the launcher application will be displayed. The launcher will only show the allowed applications where a check is performed by associating every PIN with a specific user profile. This ensures that the application launcher only loads the allowed applications for a specific user profile.

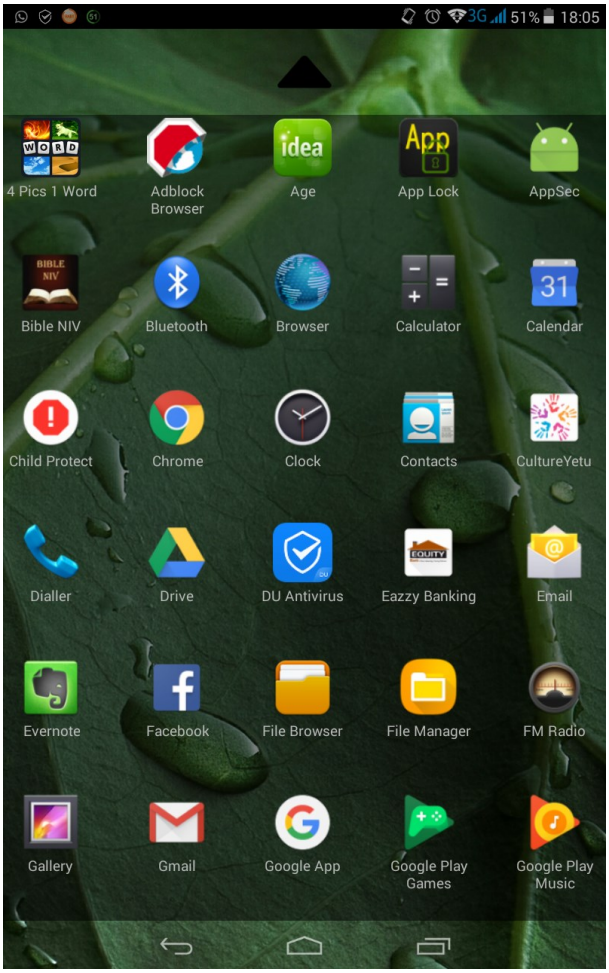

Figure 5.11: Launcher Screen

5.3 System Testing

This describes tests performed on the system to determine if it achieves the set objectives. It will further describe the different tests performed against the functional and non-functional requirements.

5.3.1 Usability Testing

This type of testing was used to determine whether the application was user friendly through checking whether the user could understand the application without interacting with it. System flow was checked to determine if the user finds it easy to navigate to the expected window and accomplish a task within minimal steps. This testing also checked whether the system icons and words were easily interpreted and understood by the user. Table 5.1 below shows some of the tests that were carried and their respective results.

Table 5.1: Application Usability Testing

Test Case	Application Usability		
Description	Test for Application Usability		
Pre-Condition	Application must have loaded successfully		
Post-Condition	Users can easily navigate through the application		
Step	**Action**	**Expected Response**	**Result**
a)	User tries to access navigation drawer and all options visible to the user.	Drawer menu is functioning and all options visible and clickable.	Pass
b)	User tries to navigate to different windows within the limited number of steps.	User must take at most three steps to get to the desired window or perform a certain function.	Pass
c)	User determines if icons and symbols used are relevant and produce the desired result.	Floating icons perform the expected purpose, drawer menu icons ease the process of identifying features and functionalities.	Pass

5.3.2 Functional Testing

Functional tests were done to determine whether the functions of the system work as per the system requirements. One of the methods used were to test based on the use cases to determine their success or failure of the system implementation and design. The main use cases were tested where

test measures were used to determine the success or failure of the result. The tables below show the test cases and their respective results.

Table 5.2: Create Account Test Case

Identifier	1
Test Case	Creating user account
Description	User creates account using their personal information
Utilised Use Case	Register
Results	Successful account creation
Pass/Fail	Pass

Table 5.3: Sign In or Out Test Case

Identifier	2
Test Case	Sign in or sign out of the system
Description	User performs logging with email and password pair then signs out.
Utilised Use Case	Login and Logout
Results	Successful login and access is granted or successful logout and Login screen is shown.
Pass/Fail	Pass

Table 5.4: Manage User Profiles Test Case

Identifier	3
Test Case	Manage user profiles
Description	User performs add, edit and delete operations on user profiles
Utilised Use Case	Manage User Profiles
Results	User profile successfully added, edited or deleted.
Pass/Fail	Pass

Table 5.5: Block Application and Settings Test Case

Identifier	4
Test Case	Block applications and settings
Description	User selects the applications to block
Utilised Use Case	Block Applications and Settings
Results	Applications blocked successfully and do not appear on application launcher.
Pass/Fail	Pass

Table 5.6: Search Application Test Case

Identifier	5

Test Case	Search for an application
Description	User searches for an application using its name
Utilised Use Case	Search Application
Results	The list only shows the searched application or relevant suggestions based on the user's input.
Pass/Fail	Pass

Table 5.7: Manage Users Test Case

Identifier	6
Test Case	Manage registered users
Description	User deletes or deactivates registered users
Utilised Use Case	Manage Users
Results	User successfully deactivates or deletes a user
Pass/Fail	Pass

Table 5.8: Generate Reports Test Case

Identifier	7
Test Case	Generate system reports
Description	System generates reports

Utilised Use Case	Generate Reports
Results	User successfully views different types of reports
Pass/Fail	Pass

Table 5.9: Phone Storage Access Test Case

Identifier	8
Test Case	Phone Storage Access
Description	Limit access to phone storage
Utilised Use Case	Block Apps and Settings
Results	User successfully blocked USB connections and file manager applications and the phone storage was inaccessible. Phone connects as charger only when connected to PC.
Pass/Fail	Pass

Table 5.10: Block Application Installation Test Case

Identifier	9
Test Case	Block Application Installation
Description	Prevent installation of new application
Utilised Use Case	Block Apps and Settings

Results	Installation of a new application prompted for an administrator password failure to which the process was aborted. Further the user successfully blocked USB Connection, USB debugging, installation of applications from unknown sources, hid applications that enable installation from application store and blocked Wi-Fi and Data services. This prevented all avenues that can be used to install new applications.
Pass/Fail	Pass

5.3.3 Compatibility Testing

This testing was done to ensure the system was compatible with existing platforms by testing the application against different Android platforms. Table 5.11 shows the result of the compatibility testing.

Table 5.11: Android Platform Compatibility Test

Android Platform	**Test Result**
Android 10 (2.3.3)	Pass
Android 11 (3.0)	Pass
Android 12 (3.1)	Pass
Android 13 (3.2)	Pass
Android 14 (3.3)	Pass
Android 15 (4.0.3)	Pass
Android 16 (4.1.2)	Pass
Android 17 (4.2)	Pass
Android 19 (4.4)	Pass

5.3.4 Load Testing

This test was performed to determine the application's performance, response time, resource utilisation and the application's breaking point. This was done by running the application on different devices and observing how the application performs, the time it takes to respond to a client's request, the phone's memory and processor utilisation and the circumstances that make the application fail. Figure 5.12 shows a screen that contains a list of applications that can be blocked or unblocked.

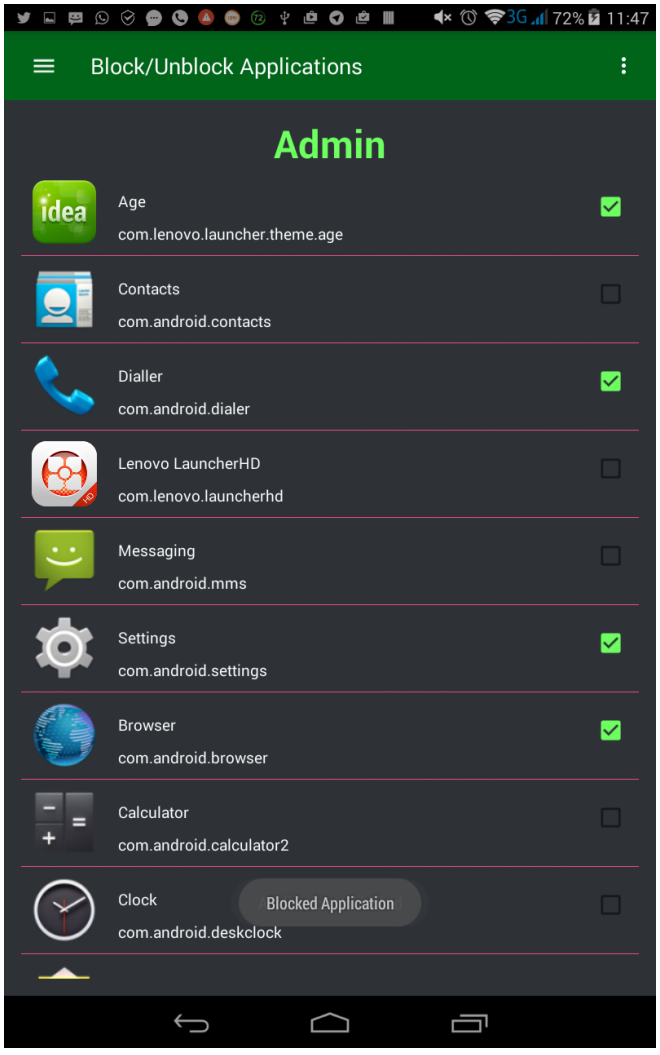

Figure 5.12: Application List with Block or Unblock Options

Table 5.12 below shows the tests that were carried out and their respective results.

Table 5.12: Load Testing

Test Case	Application Load Testing		
Description	Test for application's performance, response time, breaking point and resource utilisation.		
Pre-Condition	Application must have loaded successfully		
Post-Condition	Application performs as expected without any failure or slowness.		
Step	**Action**	**Expected Response**	**Result**
a)	CPU Utilisation: Run application and perform multiple functions while monitoring CPU usage.	Application should not exceed 2% utilisation of the CPU.	CPU utilisation varies from 0.2% when not in use to 1.6% when performing major functions.
b)	Memory (RAM) Utilisation: Run application and perform multiple functions while monitoring memory usage	Application should not utilise more than 25 Megabytes of memory.	Memory usage varies from 2 megabytes when idle to 15 megabytes when performing major functions.
c)	Response Time: Login or Register through the application and monitor the time it takes to send a request and receive a response.	The average response time should be less than 4,000 milliseconds.	Average response time is 2,567 milliseconds.
d)	Performance: Synchronise local	Application should not exceed 2% CPU usage,	An average CPU usage of 16% was recorded,

	database with the remote database and monitor the application's performance when the load is increased.	25 megabytes of RAM usage and should not exceed the response time of 4, 000 milliseconds. The application should not hang.	an average of 15 megabytes of RAM was utilised and an average response time of 3,279 milliseconds was recorded.
e)	Breaking point: Create multiple user profiles and perform simultaneous synchronisation with remote database and monitor if the application will crash	The application must at least 8 user profiles with simultaneous synchronisation with remote database. Many profiles could make the application to crash due to the inability to handle many requests and responses sent by the server.	The application supports 9 profiles effectively but crashes when an attempt to synchronise data of 10 user profiles with remote database is performed.

5.3.5 Integration Testing

Integration testing was performed through combining individual units of the system and testing the system as a whole. Table 5.13 below shows the tests that were carried out.

Table 5.13: Integration Testing

Test Case	System Integration
Description	Test for application integration with the web application.
Pre-Condition	Application must have loaded successfully
Post-Condition	Application can communicate with the web application.

Step	Action	Expected Response	Result
a)	User can register and login on the mobile application.	Successful registration and login demonstrates that the application has successfully connected with remote database.	Pass
b)	The mobile application should synchronise with the web application without the user initiating the synchronisation process.	Blocked applications stored in the phone's SQLite must be viewable from the end of the web application. The web application can perform analysis on the data received from the mobile application.	Pass

5.4 User Testing

User testing ensured the end users of the system gave feedback on the application. This information was important in determining whether the application was meeting the desired goal and to further refine the prototype so as to come up with a satisfactory system. A total of 32 respondents took part in user testing. The main areas of focus were:

i. User friendliness
ii. Functionality
iii. Acceptability
iv. Aesthetics

5.4.1 User Friendliness

This involves the ease of learning and using the system. The respondents gave feedback on the user friendliness of the application in the range of easy, average and difficult. 65% of the respondents indicated that the application was easy to use and learn. 18% of the respondents indicated it was average and the remaining 17% indicated that the application was difficult to learn and use. Figure 5.13 shows a summary of the results.

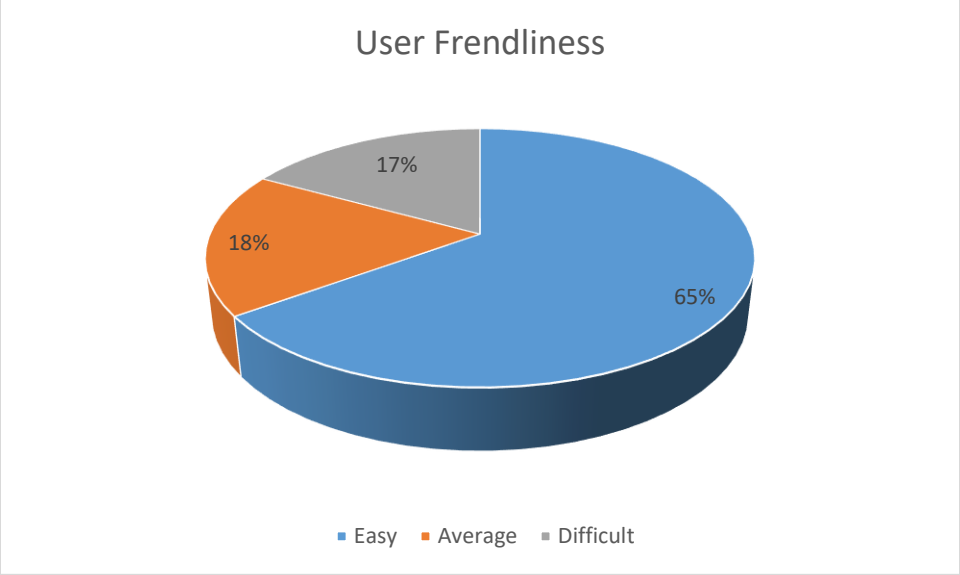

Figure 5.13: User Friendliness Feedback

5.4.2 Functionality

This involves testing the functionality of the system against the user specifications. The respondents gave feedback on the functionality after testing the application and they ranged their response from very satisfied, satisfied, neither satisfied nor dissatisfied, dissatisfied and very dissatisfied. 51% of the respondents were very satisfied with the functionality of the system, 22% of the respondents indicated that they were just satisfied, 14% of the respondents were neither satisfied nor dissatisfied, 11% of the respondents were dissatisfied and the remaining 2% indicated that they were very dissatisfied with the functionality of the system. Figure 5.14 shows a summary of the results.

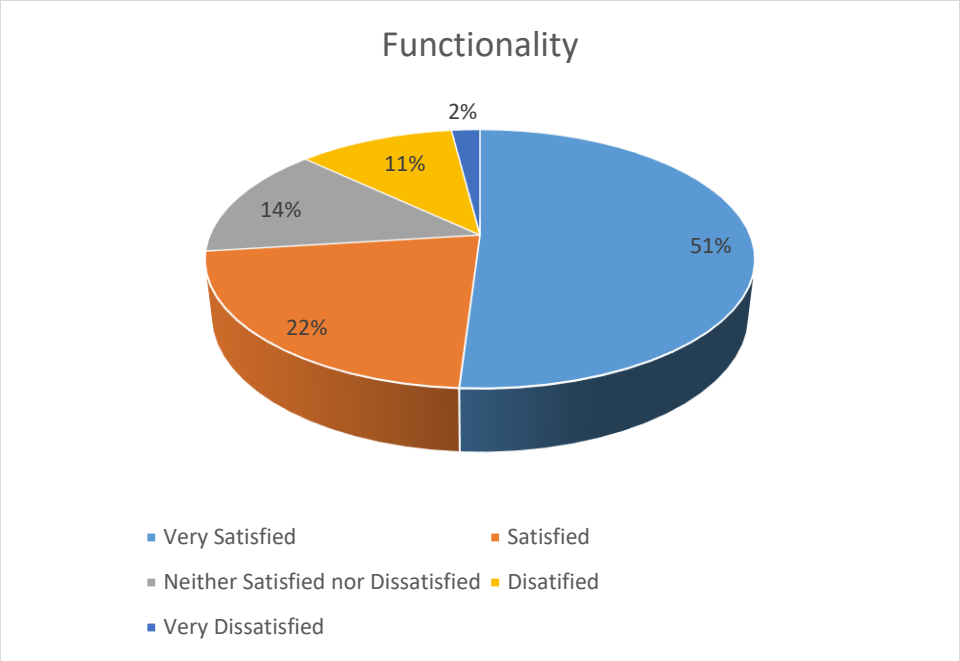

Figure 5.14: Respondent's Feedback on the Functionality of the System

5.4.3 Acceptability

This test was done to ensure that the application was a success and was well accepted by the end users. The options provided to the respondents were; accepted, undecided and rejected. 81% of the users indicated that they would gladly use the application to administer access control on their mobile devices, 15% were undecided while 4% rejected the application. Figure 5.15 shows a summary of the responses on a chart.

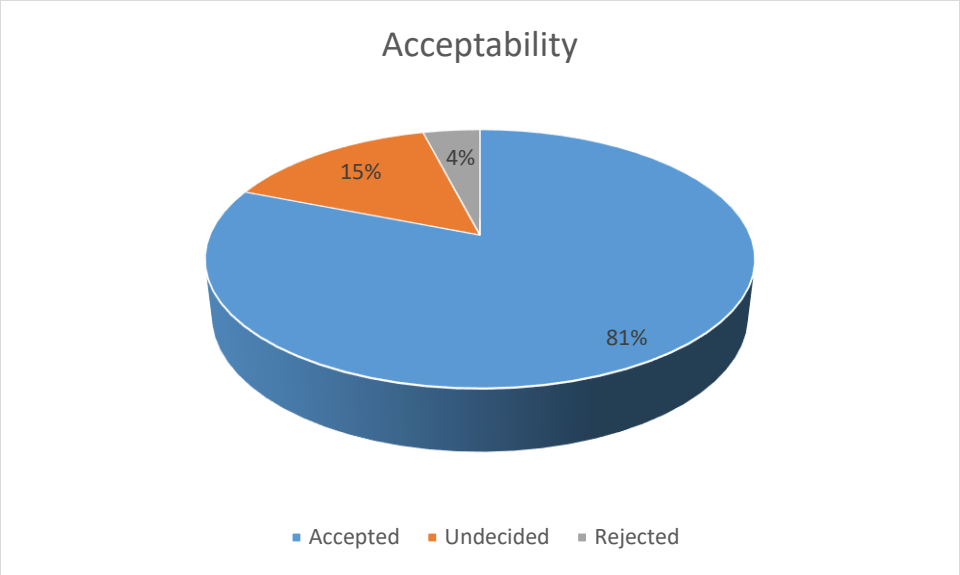

Figure 5.15: Respondent's Feedback on the Acceptability of the System

5.4.4 User Interface Aesthetics

The respondents tested the application's appearance where 79% of them found the application to be attractive, 17% of the respondents found it to be average and 4% found it to be unattractive. Figure 5.16 shows a summary of the results.

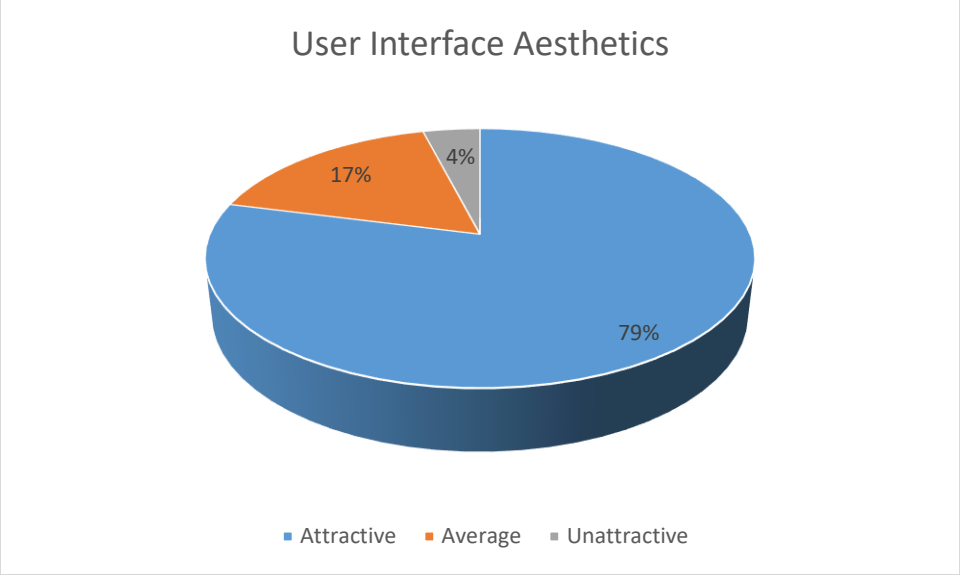

Figure 5.16: Respondent's Feedback on User Interface Aesthetics

5.4.5 Validation

Validation was carried out to determine whether the developed system addressed the challenges of administering access control on mobile devices. Respondents were to give feedback on the applicability of the solution in administering access control on their mobile devices. The respondents were asked to indicate whether the functionalities provided by the mobile application fully solves the problems that they face with the security of their mobile phones. 75% of the respondents indicated that the functionalities provided by the system fully solves the problem of security on their phones. The remaining 25% indicated that it does not fully solve the problem. Figure 5.17 shows a summary of the result.

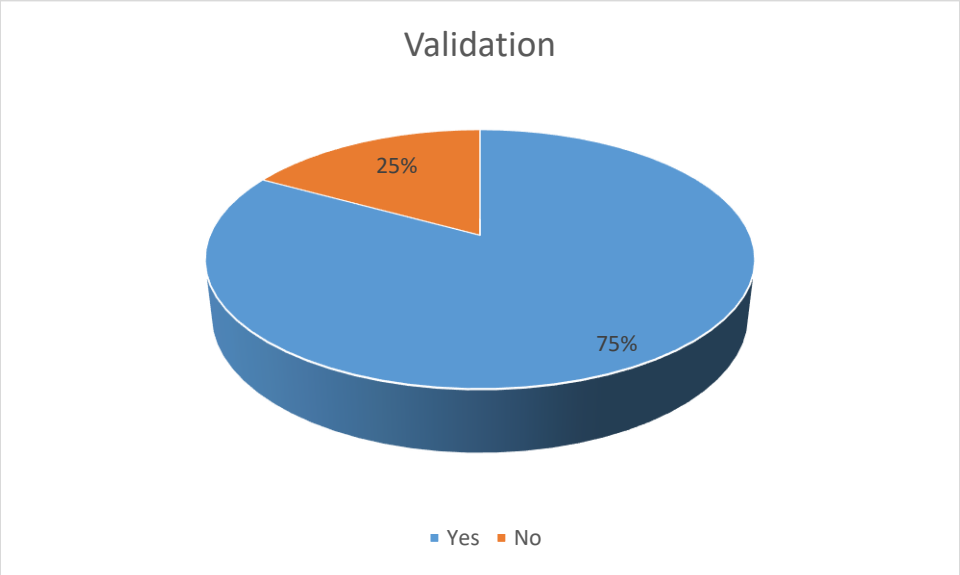

Figure 5.17: Respondent's Feedback on Whether the Mobile Application Solves the Challenges of Administering Access Control on Mobile Devices

5.5 Conclusions

Data gathered in the requirement gathering and analysis stage helped formulate system requirements that were used in system implementation. The system design phase aided in ensuring the system was implemented in the most efficient way putting into consideration the objective and research questions of the system so as to develop a system that meets the requirements of the user through achieving the objectives. The users tested the developed application and validated it to confirm that it actually performed what the users expected it to do.

Chapter 6: Discussion of Results

6.1 Introduction

The purpose of these research was to identify the challenges facing administration of access control on mobile devices, to investigate the current techniques used for administering access control on mobile devices, to design, develop and test a mobile application that administers access control on mobile devices and to validate that the mobile application actually administers the access control on mobile devices and if it solves the challenges faced by the current techniques.

The main aim of following the objectives of the research was to come up with the best solution that will identify the gap in the current techniques and ensure a suitable solution is formulated to solve the challenges faced by the current systems. A review of the existing solutions helped identify the gap faced in administering access control and further the findings of the research guided in identifying the suitable techniques to be used to come up with an application that administers access control on mobile devices. This resulted to the use of a role based approach to administer access control on mobile devices where access to specific mobile phone resources was granted based on the access rights of a specific role.

This chapter further describes the research findings and achievements, how the research objectives were obtained and reviews the developed application understanding how it was implemented and outlining its advantages and limitations.

6.2 Findings and Achievements

A review of the literature indicated that the system and techniques used to administer access control include, in-built phone features such as lock screen passwords and full system encryption and third party applications that aim to prevent the access to applications. Third party applications have placed their focus on the use of passwords to block applications where a list of passwords to be blocked is created and any attempt to block the application will prompt for a password. This approach works for limiting access to certain applications but it is limiting since there is need to only show to the person using the phone the allowed applications. Another issue is that blocking an application creates an impression that also the application resources are blocked. Connecting to the phone to a computer via USB reveals access to all the application resources which proves to be a major security gap.

This research makes improvements on the existing solutions used to administer access control by taking a different approach from the normal conventions. This approach involves using a role-based convention to administer access control where only allowed applications are displayed on the launcher.

The respondents were picked at random to give feedback on the proposed solution. 95% of the respondents owned smartphones where 65% of the respondents were using a phone with an Android platform, 13% were using a phone with an iOS platform, 8% were on a Blackberry platform, 7% were on a Windows platform and the remaining 5% were on a Symbian platform. Since majority of the respondents had Android phones, the Android platform was the preferred platform to develop the application.

The challenges faced with the current systems include: lack of a dynamic approach to implement access control with multiple accounts created for desired scenarios, access to application resources is still open through other channels despite having blocked the application, and blocked applications are still displayed on the launcher.

Based on the above findings, an access control application was designed and developed aimed at mitigating the problems present in the existing solutions. The application targeted the Android platform. Some of the features of the application includes: creation of different user profiles and a single profile contains a list of blocked and allowed applications, an application launcher to display only allowed applications based on the user profile, each profile has a unique pin to access the application launcher, settings options to block access to of application data via USB connections to computers or other electronics.

The application successfully passed user testing. Tests performed on its functionality resulted to 73% of the respondents indicating that the application's functions met their specification. On tests done on the acceptability of the system 81% of the respondents indicated that they accepted the system. On tests done on user interface design, 79% of the respondents indicated that the system was attractive. The system was also validated to ensure it addressed the challenges of administering access control on mobile devices. 75% of the respondents indicated that the functionalities provided by the system fully solves the problem of security on their mobile phones.

6.3 Review of Research Objective in Relation to the Mobile Application

This dissertation identifies the challenges facing administration of access control on mobile devices, the process of administering access control and the techniques used for administering access control. A system was developed with relation to the research objectives, findings in the literature review and the system designs.

The first objective was to identify the challenges facing administration of access control on mobile devices. This was objective was analysed in the literature review where they main reasons were lack of standards for implementing access control on mobile devices and the aspect of administering access privileges on mobile phones. In other systems, access control is mainly implemented using a role-based approach where each role contains an access list. The access list is where access rights are implemented. The system was developed to address the mentioned challenges.

The second objective was to investigate the existing techniques and mechanisms used to administer access control on mobile devices. A review of the existing technologies was done and it helped the researcher identify the gaps that exist in the existing techniques and which existing solution has a working solution but requires improvements. This also helped the researcher have an idea on the designs to use when design the proposed solution. The existing techniques include: in-built phone features such as lock screen passwords and full system encryption and third party applications which use passwords to block a list of applications.

Based on the existing technologies, the best approach was to develop a launcher application that only loads a list of allowed applications. The launcher will be accessed using a PIN linked to a user profile. Different user profiles will have different PINs and each will load different applications on the launcher depending on the access list. The phone owner will have an interface where administrative functions will be performed.

The third objective was to design test and develop a mobile application which will administer access control on mobile devices. The objective was achieved through the design, implementation and testing of the mobile application. Some of the tests carried out include: Load testing, compatibility testing, functional testing and user testing which entails tests on user friendliness, application's functionality, aesthetics and user acceptance.

The fourth objective was to validate the mobile application to check whether it addresses the challenges of administering access control on mobile devices. The respondents were requested to give feedback on whether the developed solution enables them administer access control on mobile devices. 75% of the respondents indicated that the developed application fully provides access control functionalities on their mobile devices while the remaining 25% felt that it does not fully administer access control on their mobile devices.

6.4 Review of the Application in Relation to the Current Methods Used to Administer Access Control on Mobile Devices

The proposed system is an Android application for administering access control on mobile devices. The application is a launcher application takes control of the whole phone activities. These launcher application only displays the allowed applications. The current methods of administering access control methods involves the use of a single password that blocks a list of applications. Access to a certain application will prompt for a password.

The developed application incorporates a launcher which only loads applications based on the settings specified in the user profile. The proposed application makes use of a role-based approach where different user profiles can be used to access the launcher application with each profile having its own access list. The access list lists all the applications that have been blocked or unblocked. This approach ensures the phone owner to define different profiles with different PINS. A different individual will be given a PIN which is linked to a guest account which will only display allowed applications linked to the guest account.

The current applications only focused on blocking applications without much focus on the application data. Application data is easily accessible to anyone who has access to the mobile phone's storage. Therefore, the current application solves that problem by only allowing the administrator who is the phone owner, access to the storage. Connecting the phone to a computer via USB will not grant access to the phone's storage not unless the phone owner enables USB access in the application settings.

6.4.1 Advantages of the Application

Advantages of the application in relation to the current methods of administering access control on mobile devices include the following:

i. It is an application launcher which takes control of the whole application.
ii. It only displays the allowed applications. All blocked applications are hidden blocked.
iii. It makes use of a role based approach in administering access control.
iv. It creates different profiles for different users and blocks applications based on a single profile.
v. It secures access to the phone storage only giving rights to the phone owner.
vi. It gives the phone owner more control over their mobile phones.
vii. It gives control over the installation of new applications.

6.4.2 Limitation of the Application

The limitations of the application include the following:

i. The mobile application can only be used with smart phone users who have an Android phone.
ii. The mobile application requires Internet connectivity during registration and administrator login and also when receiving reports from the backend system.

Chapter 7: Conclusions, Recommendations and Future Work

7.1 Conclusions

Mobile phones are currently being used to perform various activities and this leads to the use of applications that handle sensitive data and some of these data is stored on the mobile phones. Information gathered on how to secure these applications and their data resulted to the use of access control mechanisms to determine who can access applications and their data. A review of the current methods being used was done and an analysis of the findings noted that there is a problem in how the current methods administer access control on mobile devices.

The major gap was that application data was still accessible to anyone despite the applications being blocked and also there is need to only show what is necessary which means blocked applications should not be visible on the phone's application launcher. Another gap identified was the inability of the current methods to administer access control based on the user accessing the phone. This can be easily achieved by using a role based approach to administer access control.

The result was the development of a mobile application that administers access control with an aim of solving the problems of the existing solution. The key features of the application include:

i. An application launcher that takes control of the phone.
ii. Creating different user profiles and assigning a unique PIN to each user profile.
iii. Blocking applications based on a user profile.
iv. A lock screen that requests for a PIN and only opens the launcher when the correct PIN is entered.
v. Application launcher only loads the allowed applications associated with a user profile.
vi. Blocks access to phone storage via USB connections.

The application was tested and validated by users and their feedback proved that the application passed both the system and user testing and further the users accepted that the application solves the problems that they face with the security of their mobile phones.

7.2 Recommendations

Securing access to applications and their data is very important since it will prevent exposure of sensitive or harmful content to the wrong individuals. Therefore, my recommendation for the application to work better is, firstly, the application must be set as the default launcher application of the mobile phone so as to take control of the whole phone. Secondly, the phone owner should only administer full rights to the administrator profile but limit access to the other profiles.

7.3 Future Work

Despite all the solutions provided in this research, the solutions can be improved to make the make the process more secure and efficient. This is attainable because, technology is continuously improving and mobile phones with new advance features and capabilities are being released on a daily basis that could further even more discoveries. Therefore, the following are areas that could be explored in future to improve this solution.

i. Segregation of user accounts to ensure data for each application is defined and stored independently for each user account. This is a similar concept to OS of computers where each user account uniquely has its own data, settings and features without affecting other user accounts.
ii. Performing a remote wipe in case the mobile phone is lost or stolen where the next time the mobile phone connects to the Internet, the mobile phone will undergo a factory reset. This is mainly to ensure the data stored on the mobile phone is completely destroyed when the phone cannot be found.
iii. Developing iOS and Windows Mobile version of the application to target users using phones that run these operating systems.
iv. Implementing encryption so as to ensure security of data stored on the phone in case of theft or misplacement.

References

Ambler, S. (2014a). UML 2 Class Diagrams: An Agile Introduction. Retrieved 22 April 2017, from http://www.agilemodeling.com/artifacts/classDiagram.htm

Ambler, S. (2014b). UML 2 Use Case Diagrams: An Agile Introduction. Retrieved 22 April 2017, from http://www.agilemodeling.com/artifacts/useCaseDiagram.htm

App Review : AppLock (DoMobile Labs). (2016, May 12). Retrieved 11 January 2017, from https://softwarepen.wordpress.com/2016/05/12/app-review-applock-domobile-labs/

Arora, H. (2012, July 18). Introduction to Cryptography Basic Principles. Retrieved 23 April 2017, from http://www.thegeekstuff.com/2012/07/cryptography-basics

Bell, D. (2004, February 16). The sequence diagram. Retrieved 22 April 2017, from http://www.ibm.com/developerworks/rational/library/3101.html

Boyles, J. L., Smith, A., & Madden, M. (2012, September 5). Privacy and Data Management on Mobile Devices. Retrieved 23 April 2017, from http://www.pewinternet.org /2012/09/05/privacy-and-data-management-on-mobile-devices/

Brachman, B. (2006, December 13). Rule-based access control. Retrieved 23 April 2017, from http://www.ibm.com/developerworks/library/ws-soa-access/index.html

Brandewie, R. (2009, August 24). New challenges for access control. Retrieved 11 January 2017, from https://www.scmagazine.com/opinions/new-challenges-for-access-control/article/ 556281/

Chen, H., & Sivakumar, T. (2005). Access control for future mobile devices. In *Wireless Communications and Networking Conference, 2005 IEEE* (Vol. 3, pp. 1527–1532). IEEE. Retrieved from http://ieeexplore.ieee.org/abstract/document/1424741/

Cooney, M. (2012, September 21). 10 common mobile security problems to attack. Retrieved 11 April 2017, from http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

Fawcett, K. (2014, May). The Future is Here: What's Next For Mobile Phones? Retrieved 23 April 2017, from http://www.smithsonianmag.com/smithsonian-institution/the-future-is-here-whats-next-for-mobile-phones-180951479/

Funamo! Best Mobile Parental Control for Android Cell Phones, Tablets! (2015). Retrieved 11 January 2017, from https://www.funamo.com/

Gaur, P. (2015). Access control security features | Cyber Security Community. Retrieved 24 April 2017, from https://securitycommunity.tcs.com/infosecsoapbox/articles/2016/07/21/access-control-security-features

IBM Knowledge Center - Discretionary access control (DAC). (2014). Retrieved 23 April 2017, from https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha700/icha700_Discretionary_access_control__DAC_.htm

IBM Knowledge Center - Mandatory access control (MAC). (2014). Retrieved 23 April 2017, from https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibmzos.v2r1.icha700/icha700_Mandatory_access_control__MAC_.htm

Implementing Security Access Control (SAC). (2013). Retrieved 24 April 2017, from http://www.agiledata.org/essays/accessControl.html

InfoSec Resources - Access Control: Models and Methods. (2012, November 28). Retrieved 11 January 2017, from http://resources.infosecinstitute.com/access-control-models-and-methods/#gref

Messer, J. (2017, April 19). Mobile Device Synchronization – CompTIA A+ 220-802: 3.5 « Professor Messer IT Certification Training Courses. Retrieved 24 April 2017, from http://www.professormesser.com/free-a-plus-training/220-802/mobile-device-synchronization/

Miessler, D. (2005, October 4). Security: Identification, Authentication, and Authorization. Retrieved 24 April 2017, from https://danielmiessler.com/blog/security-identification-authentication-and-authorization/

Myhrvold, C. (2012, August 3). Study Reveals a Confused View of Mobile Phone Privacy and Security. Retrieved 11 April 2017, from https://www.technologyreview.com /s/428656/study-reveals-a-confused-view-of-mobile-phone-privacy-and-security/

MySQL :: Top Reasons to Use MySQL. (2017). Retrieved 9 February 2017, from https://www.mysql.com/why-mysql/topreasons.html

Penwarden, R. (2016). The Rise of The Smartphone. *Fluidsurveys Whitepaper*.

Perelson, S., & Botha, R. (2004). An Investigation Into Access Control For Mobile Devices. In *ISSA* (pp. 1–10). Retrieved from https://pdfs.semanticscholar.org/d142/ 98a355f838245c18c465c1c08d52c111bf1a.pdf

Rouse, M. (2013, December). What is mandatory access control (MAC)? - Definition from WhatIs.com. Retrieved 11 January 2017, from http://searchsecurity.techtarget.com/ definition/mandatory-access-control-MAC

Rouse, M. (2014, June). What is access control? - Definition from WhatIs.com. Retrieved 11 January 2017, from http://searchsecurity.techtarget.com/definition/access-control

Rubenking, N. (2016, October 19). Bitdefender Total Security Multi-Device 2017. Retrieved 11 January 2017, from http://www.pcmag.com/article2/0,2817,2461403,00.asp

Sattarova, Y., & Kim, T. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–31.

Shebaro, B., Oluwatimi, O., & Bertino, E. (2015). Context-Based Access Control Systems for Mobile Devices. *IEEE Transactions on Dependable and Secure Computing*, *12*(2), 150–163. https://doi.org/10.1109/TDSC.2014.2320731

Shelly, G. B., & Rosenblatt, H. J. (2012). *Systems analysis and design* (9th ed). Boston: Course Technology Cengage Learning.

Shinder, D. (2001, August 28). Understanding and selecting authentication methods. Retrieved 24 April 2017, from http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/

Singh, A. (2004, June). Access Control. Retrieved 24 April 2017, from http://www.kernelthread.com/publications/security/ac.html

Smith, S. (2013, April 8). Determining Sample Size: How to Ensure You Get the Correct Sample Size. Retrieved 2 May 2017, from https://www.qualtrics.com/blog/determining-sample-size/

Solomon, S. (2013, November 29). Top-10 Essential Challenges of Mobile Security - Checkmarx.com. Retrieved 11 January 2017, from https://www.checkmarx.com/2013/11/29/10-challenges-of-mobile-security/

Tutorialspoint. (2017). SDLC - Agile Model. Retrieved 12 January 2017, from https://www.tutorialspoint.com/sdlc/sdlc_agile_model.htm

Watson, R. N. (2013). A decade of OS access-control extensibility. *Communications of the ACM*, *56*(2), 52–63.

Wells, A. (2015, July 28). DU Privacy Vault - App Lock. Retrieved 11 January 2017, from /blog/app-reviews/archive/du-privacy-vault.html

Appendices

Appendix A: Questionnaire

Study Name: Mobile Application for Administering Access Control on Mobile Devices

Course: Masters of Science in Mobile Telecommunication and Innovation

Questionnaire: Citizens

NOTE: This is a volunteer questionnaire for the above named project under the course mentioned. Any data captured will be considered private and will not be disclosed without prior permission of the owner. All confidence rights will be strictly adhered.

(Please tick □ tick one box)

Section A: Personal Information

1. Gender

□ Male

□ Female

2. Age Group

□ 17 or younger

□ 18-20

□ 21-29

□ 30-38

□ 40-49

□ 50-59

□ 60 or older

3. Marital status

□ Married

□ Single

□ Windowed

Section B: Device

1. Do you own a phone?

□ Yes

□ No

2. What type of phone do you own?

 Feature Phone

 Smart Phone

 Others, please specify……

3. What operating system does your mobile run on?

 Windows

 Android

 iPhone (IOS)

 Symbian Phone

 Blackberry

 Others, please specify……

Section C: Phone Security Concerns

1. Are you aware of sensitive data stored on your mobile phones?

 Yes

 No

2. Do you feel if these sensitive data is leaked it can cause security breach?

 Yes

 No

3. Do you have any experience with unwanted access or security breach of data stored on your mobile phone?

 Yes

 No

4. If yes, which scenarios have led to this breach or unwanted access?

 Phone Theft

 Unauthorised access (friend, family or unknown person)

 Connecting to computer e.g. via USB

 Other, please specify……..

5. Do you think there is need to protect applications and data stored in mobile phones?

 Yes

 No

Section D: Existing Solutions

1. Are you aware of existing technologies that aim to protect phone applications and data?

 Yes

 No

2. If yes, give examples of these applications depending on the categories given below.

 Antivirus applications……..

 Parental Control Applications……..

 Applications designed specifically to block applications and phone data……...

3. What are some of the features in the above applications that are used to offer security?

 Locking the phone and using a password to access the phone.

 Block applications and use a password to access all blocked applications

 Remote wipe

 Others, please specify……

Section E: Proposed Solution

1. Would you prefer a solution that not only blocks the application but also hides it from the launcher?

 Yes

 No

2. Would you prefer to only show what you want to be seen?

 Yes

 No

3. Would you prefer a solution that creates user profiles and only displays certain applications for every user profile?

 Yes

 No

4. Would you prefer a solution that enables the phone owner limit access to data by controlling developer options such as USB debugging and USB connections to laptop. Only the phone owner will have this options when he/she signs in as an administrator?

- Yes
- No

5. Would you set the proposed application as the default launcher so as to enjoy the mentioned features?

- Yes
- No

6. Will you use the proposed solution?

- Yes
- No

7. Do you think the proposed solution will achieve the goal of offering security to phone applications and data?

- Strongly Agree
- Agree
- Neither Agree nor Disagree
- Disagree
- Strongly Disagree

Thank you for taking time to provide your feedback!

Appendix B: Turnitin Report

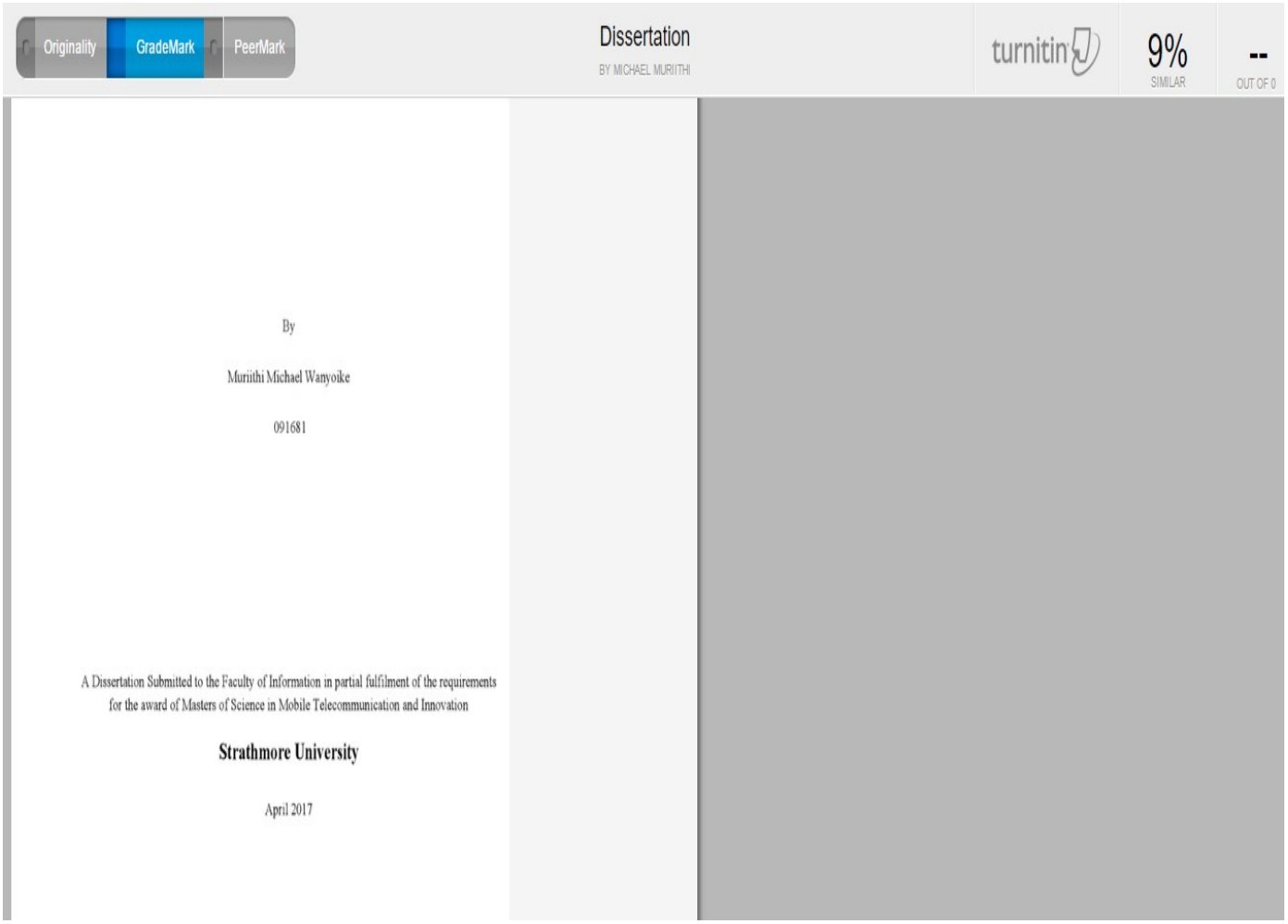

Figure B1: Turnitin Report

Appendix C: Application Screenshots

a) Registration Screen

This screen ensures phone owners register as system users. This enables users to get login credentials which will be used to gain access to the system. Figure 5.1 shows the registration screen for the system.

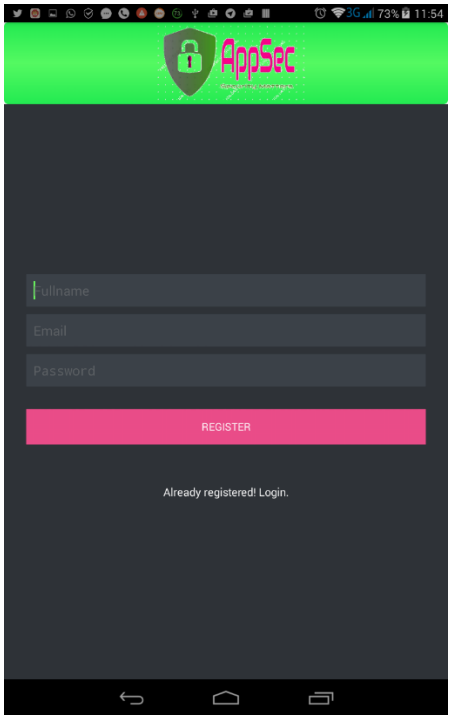

Figure C1: Registration Screen

b) Login Administrator Screen

This is screen will be used by phone owners to gain access to the system. Only a single account can be used to login into the system for each mobile phone. This ensures that only the phone owner's account is associated with the mobile phone. Figure 5.2 shows the login screen to be used by phone owners to access the system.

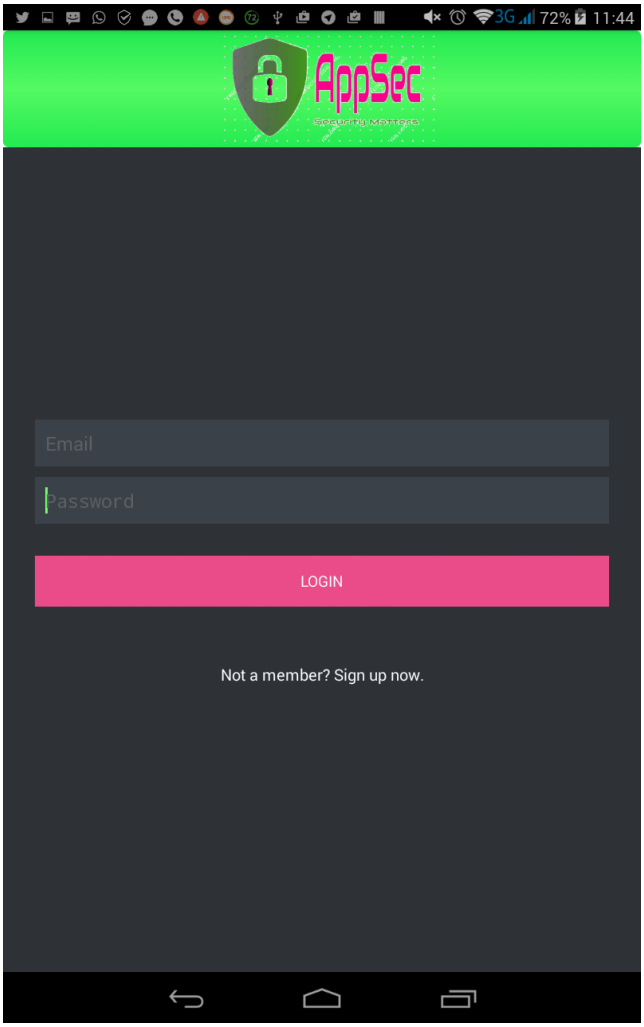

Figure C2: Login Screen