KWAME NKRUMAH UNIVERSITY OF SCIENCE & TECHNOLOGY (KNUST)-KUMASI

DEPARTMENT OF COMPUTER SCIENCE

A COMPARATIVE STUDY OF REMOTE ACCESS TECHNOLOGIES AND IMPLEMENTATION OF A SMARTPHONE APP FOR REMOTE SYSTEM ADMINISTRATION BASED ON A SECURE RFB PROTOCOL

BY

GANAA DOMANAANMWI ERNEST

(BSc Computer Science)

A Thesis submitted to the Department of Computer Science, Kwame Nkrumah University of Science and Technology in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

In Information Technology,

College of Science

NOVEMBER, 2015

CERTIFICATION

I hereby declare that this submission is my own work towards the MSc in Information Technology and that, to the best of my knowledge; it contains no material previously published by another person or material which has been accepted for the award of any other degree elsewhere, except where references have been made and duly cited in the text.

GANAA DOMANAANMWI ERNEST ………………………………….. ……………………………………
(Student PG8299912) Signature Date

Certified By:

Mr. FRIMPONG TWUM ………………………………….. ……………………………………
(Supervisor) Signature Date

Certified By:

Dr J. B. Hayfron- Acquah ………………………………….. ……………………………………
(Head of Department) Signature Date

DEDICATION

This thesis is dedicated to God for His awesomeness and to my lovely wife and daughter for their love and care in my life.

ACKNOWLEDMENT

I deeply appreciate God, for the gift of life and His faithfulness in seeing me through my master's programme.

Special thanks to my Supervisor, Mr. Frimpong Twum for providing the research direction for this work and for his immense suggestions especially towards the completion of the work. He really demonstrated his skills and experience in providing research guidelines all through the work.

Thanks to my senior colleagues Mr. Kwasi Antwi Danso and Mr. Richard Osei Sakyi both of Wa Polytechnic ICT department for their support and encouragement anytime there was the need.

I am also grateful to Roland Dunee for the support he provided throughout the duration of this research work.

I also wish to thank my family, especially my siblings for helping me to imbibe the values of education early in life and all the sacrifices of childhood training. Finally, I appreciate my lovely wife Victoria Dunee and my wonderful daughter Viola Ganaa who have all contributed immensely to my fulfilment in life.

LIST OF ABBREVIATIONS

RDP	Remote Desktop Protocol
RFB	Remote Framebuffer protocol
ICMP	Internet Control Message Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
MITM	Man-In-The-Middle
SSL	Secure Socket Layer
SMS	Short Messaging Service
PHP	Hypertext Pre-Processor
VPN	Virtual Private Network
App	Application
VNC	Virtual Network Computing
UDP	User Datagram Protocol
SMTP	Simple Message Transfer Protocol
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
ARP	Address Resolution Protocol
DoS	Denial of Service
DNS	Domain Name Service
SSH	Secure Shell Protocol
TLS	Transport Layer of Security
OTP	One Time Password

RD	Remote Desktop
OS	Operating System
SRD	Software Requirement Document
URD	User Requirement Document
XAMPP	Cross-platfrom, Appache HTTP Server, MySQL, PHP and Pearl
CA	Certificate Authority
SRFB	Secure Remote Frame Buffer
WRA	Windows Remote Assistance
TV	TeamViewer
PPP	Point-to-Point Protocol

Table of Contents

DEFINITION OF TERMS

Remote Access: it is the connection to a system from a secondary location other than that of the primary location of the system being accessed.

RFB protocol: it is a simple protocol for sending graphics to be displayed on a remote client.

RDP protocol: it is a proprietary protocol designed by Microsoft for remote input and display of host running windows operating systems which is based on the Multipoint Application Sharing (T.128) recommendation by Telecommunication Union.

Self-signed SSL certificate: is a certificate signed by the individual who created it rather than a trusted Certificate Authority (CA).

Secure RFB protocol: an RFB protocol with a self-signed certificate incorporated.

Virtual Network Computing: a cross-platform application based on the RFB protocol that can be used to take control of a remote computer over a network.

Client Computer: a computer that accesses services made available by a server

Remote Server: a computer that provides services to other computers on a network and allows users to gain access to it from a remote location or a secondary location.

Virtual Desktop: a user’s desktop that comes from the server.

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

The study uses remote technologies to provide tremendous support for network administrators by implementing a secure remote system administration application that runs on android smartphones to aid them administer their servers remotely when they (network administrators) are out stationed using their smartphones.

The android app developed in eclipse establishes a secure connection with a remote server running a PHP application. The app was developed based on the RFB protocol. The RFB protocol, a display protocol has some security lapses including being vulnerable to Man-InThe-Middle (MITM) attack using a few tools and techniques. This research therefore incorporated a self-signed Secure Socket Layer (SSL) certificate in the android app to enable secure encrypted connections to be established between the android app and the remote server to ensure end-to-end security against attacks such as Man-In-The-Middle (MITM).

The whole system was deployed based on client-server architecture with the hand-held smart devices as clients, providing real-time network access to network administrators to their remote servers.

The secure RFB protocol proposed and implemented in the android app was compared with other existing software for remote administration such as RDP and RFB protocols using ICMP ping command.

CHAPTER ONE

1.1 INTRODUCTION

It is very easy for a computer network administrator to administer and monitor a network while in the office. But what happens if the network administrator is away from office? How will he or she administer or manage the network? How will the administrator even monitor and know the status of the network? These and several other issues are a matter of concern to this research.

This research looks at remote access technologies and how to implement a smartphone app for remote system administration so as to create some kind of virtual office(s) for System Administrators who will like to always be tied up to their networks even if they are out stationed.

Also, it is not a question of whether a remote access software will be used, but which one of the available remote access software will be selected by users and how the selected product will be configured to minimise security risk. It is against this background that a comparative study on remote access technologies and software has to be conducted in order to identify the strengths and weaknesses of these remote access technologies and how these weaknesses if any can be addressed.

It is hoped the findings of this research might enable system administrators' better monitor the status of their networks through using the proposed smartphone app and short messaging system (SMS) to perform system administration task as

- ✓ Remotely creating users or adding users to their networks using their smartphones
- ✓ Creating and saving text files on a remote server running a Hypertext Pre-Processor (PHP) program
- ✓ And as well read and modify text files on a remote server using their smartphones.

This research work intends to build an android mobile app based on a proposed secure RFB protocol sitting on a mobile device that will communicate with a network server running a Hypertext Pre-Processor program.

The server will perform the processing and send response back to the android app. As an example, android app will be responsible for issuing basic commands like creating files and as well as performing basic server management task such as creating users, setting user privileges, etc.

There will also be a database to keep track of users who log onto the system through their smartphones for audit trail purposes.

The structure of the system will be as shown below in figure 1.

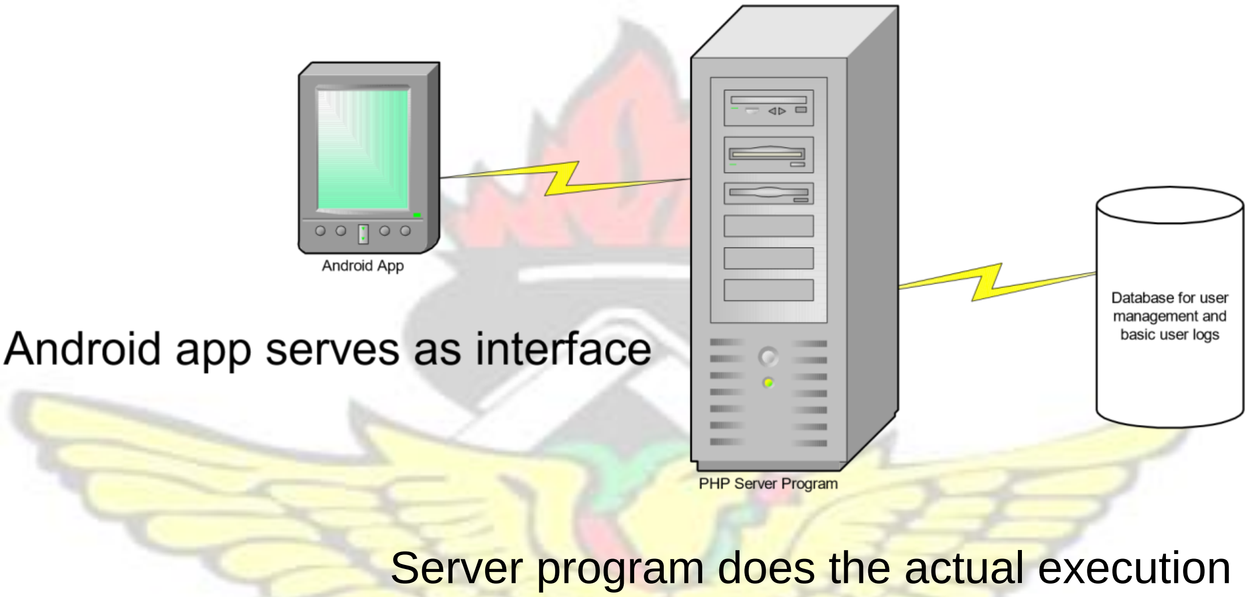

Android App
PHP Server Program
Database for user management and basic user logs
Android app serves as interface
Server program does the actual execution

Figure 1: System's architecture. Source: Author's Construct

1.2 PROBLEM STATEMENT

It has been observed that network administrators rely heavily on third party information to know the status of their computer networks any time they are away from office. This often leads to misinformation.

There is the need to allow network administrators to go beyond relying on third party information concerning their networks to be able to monitor and even administer their networks through their smartphones when out of office.

1.3 AIM OF RESEARCH

The aim of this research is to do a comparative study of remote access technologies and implement a smartphone app for remote system administration based on a proposed secure RFB protocol.

The specific objectives are as follows:

- ✓ To investigate what remote access technologies are available
- ✓ To examine the current usage of remote access technologies
- ✓ To evaluate the security of current remote access technologies
- ✓ To implement a smartphone app for remote system administration based on a proposed secure RFB protocol
- ✓ To evaluate the performance of current remote access technologies

1.4 RESEARCH QUESTIONS

The main research questions for this research work are;

- ✓ What remote access technologies are available to system administrators?
- ✓ How are these remote access technologies used by system administrators?
- ✓ How secure are current remote access technologies?
- ✓ In relation to performance, how do current remote access technologies compare?

1.5 IMPORTANCE OF INVESTIGATION

One cannot down play the value that will be derived from network administrators monitoring the status of their networks through their smartphones whenever they are away from office.

This research is very important to the extent that it will enable System Administrators monitor their networks remotely through their smartphones instead of relying on third party reports which may not even be accurate.

The researcher after completing this work will also be able to recommend to system administrators and related computer professionals which remote access software is reliable, secured and effective to use. The research will compare the response time of the RDP protocol, the RFB protocol and the secure android.

The investigation upon its completion will also allow System Administrators be able to remotely access files and modify them on their servers or even client machines through their smartphones.

The investigation will make system administration very convenient for the System Administrator who will just need only a smartphone to do system administration remotely. This research on completion will create a kind of virtual office for System Administrators since they can remotely administer systems using their smartphones.

1.6 THE FOCUS OF THE RESEARCH

It is not the question of whether remote access software will be used, but which one of the available remote access software available will be selected by users and how the selected product will be configured in order to minimise security risk. It is against this background that this research seeks to conduct a comparative study on remote access technologies and software in order to identity their strengths and weaknesses and how these weaknesses can be addressed.

The research will be focused on conducting a comparative study on remote access technologies and implementing a secure smartphone app that will be used to do remote system administration.

This will be done using tools such as Hypertext Pre-Processor (PHP) and Eclipse IDE. The PHP will be used to develop an application that will run on a server to be accessed by the smartphone, while the Eclipse will be used to develop an android app that will run on an android smartphone which will be responsible for issuing of commands to the server that will run the PHP application. The smartphone will just be some kind of an interface to the remote computer running the PHP program.

The research will seek to compare the response time of the RDP protocol, the RFB protocol and the secure android app through ICMP ping. It will also determine the availability of the RDP protocol, the RFB protocol and the secure android app.

The research will also evaluate the views of computer professionals on the use of existing remote access applications and their willingness to accept the new technology (smartphone app) the research seeks to implement.

1.7 SCOPE AND LIMITATIONS

A comparative study of remote access technologies will be conducted and a smartphone app based on a secure RFB protocol will be implemented.

In conducting the comparative study of the remote access technologies, the views of computer professional will be evaluated through questionnaires on the use of existing remote access technologies and applications.

It will also allow system administrators use their smartphones to remotely monitor their computer networks through Short Messaging System (SMS). System administrators will get SMSs on regular bases to update them on the status of their networks.

At the completion of this research work, system administrators will be able to remotely logon to a server and be able to create users or add users to their networks using their smartphones. There will also be a database to keep track of users who logon to any server remotely for audit trail purposes.

The research will seek to compare the response time of the RDP protocol, the RFB protocol and the secure android app through Internet Control Message Protocol (ICMP) ping. The availability of the RDP protocol, the RFB protocol and the secure android app will also be established.

System administrators can also remotely shutdown remote computers running a PHP program by the use of a smartphone.

System administrators also have the chance of reading text files on remote computers using their smartphones in case they are out of office but needs some information from the remote system or computer.

The research will also compare the security of RDP protocol and RFB protocol; identify their strengths and weaknesses how those weaknesses can be addressed if any.

1.8 THESIS ORGANISATION

The rest of the thesis is organised as follows: Chapter two reviewed related literature on remote access technologies and remote access applications, methodology, research design, modelling, requirements for the system developed in this thesis and the design of the system itself are presented in chapter three.

Chapter four presents the data analysis and implementation details of the system developed in this thesis, and finally, the summary, conclusion and recommendation of the thesis is presented in chapter five.

1.9 SUMMARY

This chapter started with an introduction to the chapter which gives an overview of the research and the system structure or architecture. The chapter also looked at the problem statement to justify why the research must be undertaken.

It went further to look at the aim and objectives of the thesis and even what benefits users will derive from this research after its completion. The chapter also looked at the focus of the research; here we saw how the researcher intends to conduct the research or investigation.

The chapter further looked at the scope and limitations of the research, which is what the research intends to cover and what it does not cover.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter looks at existing technologies for remote access systems and the various remote access systems available to users and what each remote access system is used for.

Remote access is the connection to a system from a secondary location other than that of the primary location of the system being accessed (Lahaie, 2013).

Some existing remote access technologies investigated are:

1. Remote Frame Buffer (RFB) protocol
2. TCP/IP protocol
3. Remote Desktop Protocol

Some of the remote access systems investigated are as follows:

- ✓ COMPROID-Remote Desktop Access through Android Mobile Phone
- ✓ Ultra VNC (Virtual Network Computing)
- ✓ Remote Computer Access through Android Mobiles
- ✓ TeamViewer
- ✓ LogMeIn
- ✓ Remote Control System
- ✓ Remote Desktop
- ✓ Windows Remote Assistance
- ✓ SMS based Remote Control System

The chapter looks at each of these remote access systems, compares them with one another, indicates their strengths and weaknesses and goes further to compare each with the system this research intends to implement.

The chapter ends with a summary or brief explanation of whatever the researcher looks at in this chapter.

2.2 EVALUATION OF EXISTING REMOTE ACCESS TECHNOLOGIES

All remote access systems or applications are developed based on existing and or appropriate technology or technologies. Some existing technologies available for developing remote access systems or applications are:

2.2.1. Remote Frame Buffer (RFB) protocol

The RFB protocol is a simple protocol for sending graphics to be displayed on a remote display or screen. RFB protocol places very little demand on the remote display in terms of processing power and memory demands since all processing is done at the server side. This protocol is a true thin client protocol because it has very low bandwidth requirements and shifts all processing demands to the RFB server instead of the RFB client (Kerai, 2010). The major interest in designing this protocol is to make very few requirements of the client in terms of processing (Richardson, 2010).

The two remote endpoints in the RFB protocol are referred to as the RFB client or viewer and the RFB server (Baig et al., 2012). The RFB client is the remote display. It works by simply taking rectangles of screen data from the RFB server with a given position and size and puts them into its frame buffer so that they appear in the correct place on the RFB client's screen (Masthan et al., 2013).

There are three stages to how the RFB protocol works. First is the handshaking phase, the purpose of which is to agree upon the protocol version and the type of security to be used. The second stage is an initialization phase where the client and server exchange ClientInit and ServerInit messages. The final stage is the normal protocol interaction. The client can send whichever messages it wants, and may receive messages from the server as a result.

Despite the fact that RFB protocol uses encrypted passwords and network, any communication over the network is vulnerable and can be attacked by a Man-In-The-Middle (MITM) by using a few tools and techniques (Kerai, 2010). Also, the applications of VNC which are developed based on RFB protocol are generally slower, offer fewer features and security options than Remote Desktop (RD) which is based on the RDP protocol (Masthan et al., 2013).

The input side of the protocol is based on a standard workstation model of a keyboard and multi-button pointing device. Input events are simply sent to the server by the client whenever the user presses a key or pointer button, or whenever the pointing device is moved.

Virtual Network Computing (VNC) was developed based on the RFB protocol (Baig et al., 2012).

One advantage of the RFB protocol is its ability to place very little demand on the RFB client in terms of processing power and memory demands since all processing is done at the server side. For this reason, the RFB protocol is good for thin clients and smartphones.

Another advantage of the RFB protocol is that it is cross-platform or platform independent and it is compatible with any operating system (Masthan et al., 2013).

One other outstanding advantage of this protocol is its ability to operate under any reliable transport such as the TCP/IP protocol (Kerai, 2010).

Despite its advantages, one disadvantage of this protocol is that, if several RFB clients are making requests to the same server at the same time, it makes the server's response time usually bad.

2.2.2 Transmission Control Protocol/Internet Protocol (TCP/IP) Protocol

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite used for communication which has become the industry-standard method of interconnecting hosts, networks, and the Internet. As such, it is seen as the engine behind the Internet and networks Worldwide (Parziale et al., 2006). The simplicity and power of this protocol has made it the single network protocol of choice in the world, and with a design goal to build and interconnection of networks referred to as an internet that provided communication services over heterogeneous physical networks. A clear benefit of TCP/IP protocol is the enabling of communication between hosts on different networks which may or may not be separated by a large geographical area.

The security of TCP/IP is based on three modules which are the security policy, security control and data security layers. The security policy belongs to the application layer, the security control is located in the transport layer while the security layer is located between the transport and IP layers (Samprati, 2012). The security policy layer of the TCP/IP interacts with system administrators to define the kind of security that will be applied to data in communication; the security control layer provides the mechanism to apply the security policy defined by the administrator in the security policy module to ensure secure communications.

Another important aspect of TCP/IP is the creation of a standardized abstraction of the communication mechanisms provided by each type of network. Each physical network has its own technology-dependent communication interface, in the form of a programming interface that provides basic communication functions. TCP/IP provides communication services that run between the programming interface of a physical network and user applications. It enables a common interface for these applications, independent of the underlying physical network. The architecture of the physical network is therefore hidden from the user and from the developer of the application. The service TCP provides to the application is a connection-oriented, reliable byte stream unlike UDP which provides connectionless unreliable service to this layer (Fall & Stevens, 2011). The transport layer TCP provides the end-to-end data transfer by delivering data from an application to its remote peer.

To be able to identify a host within the network, each host is assigned an address, called the IP address. When a host has multiple network adapters (interfaces) such as with a router, each interface has a unique IP address. A TCP data header contains the source and destination port numbers and the source and destination IP addresses in the IP header which uniquely identifies each connection (Fall & Stevens, 2011).

By dividing the communication software into layers, the protocol stack allows for division of labour, ease of implementation and code testing, and the ability to develop alternative layer implementations. Layers communicate with those above and below via concise interfaces. In this regard, a layer provides a service for the layer directly above it and makes use of services provided by the layer directly below it. For example, the IP layer provides the ability to transfer data from one host to another without any guarantee to reliable delivery or duplicate suppression. Transport protocols such as TCP make use of this service to provide applications with reliable, in-order, data stream delivery (Parziale et al., 2006).

Figure 2 below shows the TCP/IP protocol stack.

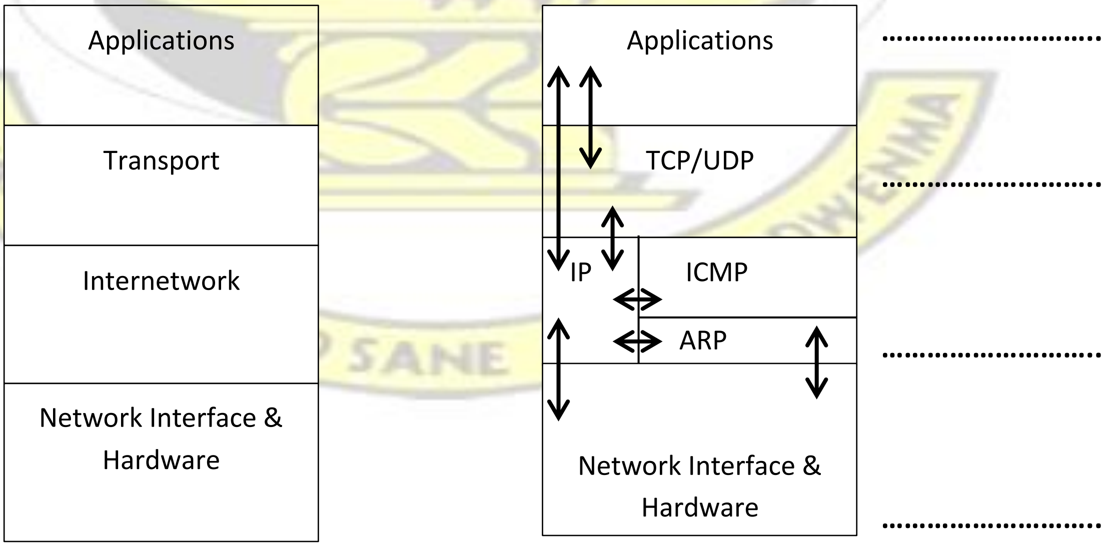


Figure 2: Shows how the TCP/IP protocols are modelled in four layers (Adopted from: Parziale et al., 2006)

The application layer is provided by the program that uses TCP/IP for communication. An application is a user process cooperating with another process usually on a different host. Examples of applications include Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP).

The internetwork layer or simply the network layer provides a virtual network image of an internet which shields the higher levels from the physical network architecture below it. The IP protocol is the most important protocol in this layer which is connectionless and does not provide reliability.

Address Resolution Protocol (ARP) which is part of the Internetwork layer is a networkspecific standard protocol used to find the MAC address of a node corresponding to a given IP address in the same subnet (Nam et al., 2012). The address resolution protocol is responsible for converting the higher-level protocol addresses to physical network addresses. These resolved addresses are stored temporarily in the ARP cache to in order to reduce the resolution time and avoid additional ARP traffic overheads.

However, ARP spoof is a security problem which poses major security threats to computer network and can even be used for Denial of Service (DoS) or Man-In-The-Middle (Behboodian & Razak, 2011). This poses major threats to

The network interface layer, also called the link layer or the data-link layer, is the interface to the actual network hardware. This interface may or may not provide reliable delivery, and may be packet or stream oriented. In fact, TCP/IP does not specify any protocol here, but can use almost any network interface available, which illustrates the flexibility of the IP layer.

TCP/IP specifications do not describe or standardize any network-layer protocols in particular; they only standardize ways of accessing those protocols from the internetwork layer.

2.2.3 Remote Desktop Protocol (RDP)

Microsoft's Windows Terminal Services was built into Windows 2000 Server, Windows Server 2003 and Windows XP's Remote Desktop to provide an easy and convenient way for

administrators to implement thin computing within an organization or for users to connect to their XP desktops from a remote computer and run applications or access files.
RDP is a proprietary protocol designed by Microsoft for remote input and display of host running the windows operating systems which is based on the Multipoint Application Sharing (T.128) recommendation by Telecommunication Union (Youming, 2013).

By default, the data that travels between the terminal server and the client is protected by the RC4 symmetric encryption algorithm which provides three levels (high level, medium level and low level) of security (Kerai, 2010). The high level security encrypts data sent from the client to the server using a 128 bit key and does same to data sent from server to client, the medium level security encrypts both data sent from client and server using a 56 bit key if the client is using at least windows 2000 and low level security only encrypts data sent from client to server using 56 bit key or 40 bit key.

According to (Montoro, 2005), though the data sent between the server and client is encrypted, the RDP protocol may be prone to Man-In-The-Middle attack because there is no verification of the identity of the server when setting up the encryption keys for a session.

The MITM attack works as follows:

- ✓ When the client connects to the server, by DNS spoofing (making a DNS entry point to another IP address than it was supposed to point to) or ARP poisoning (entering a fake IP address in a host ARP table) which causes diversion of traffic to a different host, the client is fooled to connect to the MITM instead and the MITM in turn sends a request to the server. This involves maliciously modifying the relation between an IP address and its matching MAC address (Behboodian & Razak, 2011)
- ✓ Through this the server then sends its public key, in clear text through the MITM and the MITM now sends the packet further to the client, but exchanging the public key with another one for which it knows the private part.
- ✓ The client upon receiving this sends a random salt, encrypted with the server's public key, to the MITM. The MITM decrypts the clients random salt with its private key, encrypts it with the real servers public key and sends it back to the server.

- ✓ The MITM now knows both the server and the client salt, which is enough information to construct the session keys used for further packets sent between the client and the server. All information sent between the parts can now be read in clear text.

This vulnerability occurs because the client by no means will try to verify the public key of the server. In other protocols such as the Secure Shell protocol (SSH), most client implementations solve this MITM attacks by allowing the user to answer a question whether a specific server's key fingerprint is valid (Montoro, 2005).

Microsoft confirmed the above problem and fixed the new versions of Remote Desktop Clients. Recent clients now check the Terminal Server's identity to verify its public key before allowing connections. The implication of this is that Remote Desktop has a very strong security, but of course, as time passes by, attackers develop more sophisticated tools to break through. (Nam, et al., 2012) also stated that ARP (Address Resolution Protocol) poisoning can be resolved by delivering the public key and the MAC address of the server to the client, however this is to set by the network administrator manually.

Another solution to this problem is for Microsoft to keep a list of known server keys at the client-side, alerting the user if one of the expected key is changed. Although this does not prevent MITM attacks, it can give to the user, the opportunity to check for unusual activities. Remote Desktop Protocol (RDP) 6.0 supports Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols which encrypt data sent between a server and a terminal server client (Boling, 2007). Quite a number of the Windows operating system such as Windows Server 2003 SP1, Windows Server 2008, Windows XP, Windows Vista, Windows 7 and Windows 8 support SSL/TLS for RDP 6.0.

Despite the MITM security problem, RDP is designed to support different types of network topologies, multiple LAN protocols and just like VNC, RDP works on TCP/IP connections (Kerai, 2010).

2.3 REMOTE ACCESS SYSTEMS OR APPLICATIONS

Several applications are available for the purpose of connecting to computers on a network remotely. Some of such applications are as stated below;

i. COMPROID-Remote Desktop Access through Android Mobile Phone

ii. Ultra VNC(Virtual Network Computing)

iii. Remote Computer Access through Android Mobiles iv. TeamViewer

v. LogMeIn

vi. Remote Access with ShowMyPC.com

vii. Remote Control System

viii. GoToMyPC

ix. Remote Desktop

x. Windows Remote Assistance

xi. SMS based Remote Control System

The functions provided by Compdroid are screen capture, application shortcuts, keyboard shortcuts and file transfer. The system is based on client server architecture where the client sends request to the server and waits for a response.

With the Compdroid app, when a user wants to access a remote system, the user runs the Compdroid application on his or her android phone and broadcast the request to establish the connection on the network using an IP address and the server whose IP address matches the broadcasted IP address will accept the request (Inamdar et al., 2013). Then the said server sends a One Time Password (OTP) message for authentication to the client and when it is validated a connection is then established between the server and smartphone.

In terms of technology, Compdroid is using the TCP protocol and One Time Password (OTP) to provide security. Both applications (Servlets and Compdroid) are developed in Java, Net beans on server and eclipse on client.

As can be seen from the above, Compdroid is limited to only desktop access and the One Time Password security is using is very vulnerable to security threats, however, this research goes beyond desktop access to remote system administration and also incorporates selfsigned SSL certificate in the android app which provides better security than the OTP.

VNC is a cross-platform application that can be used to take control of a remote computer over a network (Baig et al., 2012). The technology underlying the VNC system is a simple protocol for remote access to graphical user interfaces. The protocol will operate over any reliable transport such as TCP/IP (Richardson et al., 1998). VNC consists of two components which are VNC Server and VNC Viewer.

To be able to connect to a host computer and control the host from the client, VNC Server must be running on the host computer and the VNC viewer must be running on the client computer. When VNC Viewer accesses a host computer, the client computer mouse and keyboard are shared with the host computer (VNC User Guide, 2012).

When two computers (the client computer and host computer) are connected, the user can print host computer files to a local printer, transfer files between client and host computers, copy and paste text between client and host computer and even chat.

In terms of technology, VNC system is based on RFB (Remote Frame Buffer) protocol to transmit all information between connected devices (Inamdar et al., 2013).

From the above, one can clearly see that VNC is more or less a remote solution support software but not an application specialised for remote system administration purposes.

Also, you have to install the viewer in the client computer, which still demands that you are nearer to a computer or even have the right to installation on such computers.

VNC therefore falls short of functionality when a System Administrator finds himself or herself on a journey or in a remote village where there is no electricity not to talk of having access to a computer to do this kind of remote connection. However, with this research, the System Administrator only needs a smartphone but not a computer to do remote connections to remote computers.

(Chintalapati & Srinivasa, 2012) in designing a remote computer access through android built it based on the VNC protocol which is actually the RFB protocol. Their system was to allow desktop sharing, text input, pointing and clicking.

However, before a user could do any of these to a remote computer, VNC server was to be installed on a remote computer and their app which was built using java installed on a smartphone. A user will be required to enter a user name, a password and the IP address of the remote computer to be accessed.

This system can also be used for file transfer, controlling remote desktops over the internet and also for accessing applications running on remote computers, however, it does not extend to remote system administration.

The security of their system also leaves much to be desired as compared to the security (the self-signed SSL certificate) that will be incorporated into the android app this research is implementing.

TeamViewer is an intuitive, fast and secure application which is used for collaborative works. It can be used to provide ad-hoc remote support to colleagues, friends and or customers.

While many features of TeamViewer are good, there are however many of its features too which are not good from the security viewpoint (Groš, 2011). The most dangerous of these features is the possibility to completely bypass its firewall control.

TeamViewer works by using a globally unique ID which is generated based on hardware features. This unique ID is permanent and does not change later.

TeamViewer is a very good tool for collaborative work, holding meetings between individuals or groups who are in different geographical locations and basically sharing files as compared to this research which looks at remote technologies comparatively and turning a smartphone into a tool that can be used to do remote system administration.

LogMeIn provides services ranging from downloadable applications to providing helpdesk solutions which are accessible from anywhere in the world with internet connectivity.

LogMeIn also provides some kind of cloud services which are cloud-based collaboration, IT management and customer services aimed at addressing security, management and accessibility requirements of the mobile workplace (LogMeIn Inc., 2013).

To use LogMeIn, the user must sign up for a LogMeIn ID to be able to access the LogMeIn software and services. This LogMeIn ID can be obtained by going to www.LogMeIn.com and clicking on Log In, after this, the Log in or sign up page is displayed. Follow the instruction on this page to activate your account.

When a user adds host computers to a LogMeIn, those computers can be deleted from the account later if they are no longer needed by the user. LogMeIn uses the standard web protocol (HTTP) for all its communications and encrypted connections using 256-bit Secure Socket Layer (SSL) protocol.

As much as accessing a remote computer using this technology can be beneficial, convenient and interesting, once users have to fill a registration form in order to create a LogMeIn account and add the host computer to the LogMeIn account, host computers are much prone to attacks. There is no track of who logs on to a host computer remotely for audit trail purposes which this research is going to take care of.

Also, to be able to connect to a host computer remotely using LogMeIn, it is required that the host computer be connected to the internet but with this research, the host or remote computer does not necessarily need to be connected to the internet before remote connection can be established between it and the smartphone.

Bedeschi and Vincenzetti defined Remote Control System as an Information Technology stealth investigative tool which can also be used for attacking, monitoring and infecting computers and smartphones. It is an offensive security technology. Remote Control System was developed by a company called Hacking Team in Italy by two individuals called Valeriano Bedeschi and David Vincenzetti.

This system permits passive monitoring and active control of all data and processes on selected target computers and can even take control of the endpoints, that is the target computers or smartphones it is monitoring, such computers may or may not be connected to the internet.

Remote Control System is capable of monitoring web browsing, opened or deleted files, printed documents, call history, chats, SMS and GPS information. All these monitoring can be done without the users detecting that it is even installed on their systems. It is also a cross platform application.

Although Remote Control System is a very intelligent remote tool, it is not for remote system administration purposes but rather for spying on people and intelligence gathering as compared to this research work which intends turning a smartphone into a tool that can be used for remote system administration purposes.

Remote desktop is an application that works only over a TCP/IP network such as the Internet and allows a user to control the desktop and possibly takes control of the contents of one computer from the local one (Morris, 2008).

Remote desktop application provides features like file transfer and text chat. Remote desktop is a function which was included with Windows XP Professional, to enable users to connect to other computers across the Internet from virtually any computer, Pocket PC, or smartphone. A user who has only one license for an application can make other users access it using remote desktop.

It is important to know that the computer the user will be connecting to remotely must have Windows XP Professional, Windows Vista Business, Windows Vista Ultimate or a later version of a Windows as its Operating System.

The computer the user will be using to do the connection must also have any of the above versions or a home version of Windows. Both computers must be on a wired or wireless network.

However, before a computer can be connected to using remote desktop technology, this involves configuring software on both host or local computer controlling the connection and the target or remote computer to be accessed (Baig et al., 2012). For example, that computer must have a user account with a password, an IP address and must be configured to accept remote connections.

Remote Desktop is implemented using Remote Desktop Protocol (RDP) and TCP/IP protocol. However, latest versions of Windows operating systems like Windows 8 are implementing Remote Desktop using RDP, TCP/IP and RFB protocols.

As the complexity of IT increases each day, it is important to continually deliver effective and timely help desks solutions everywhere through the most efficient means possible. Remote assistance supports text chat, computer control, voice chat and file transfer. The basic function of Remote Assistance is helpdesk type activities where one experienced user remotely assists another user (BigFix Inc., 2007).

Windows Remote Assistance is Microsoft's built-in web based troubleshooting facility, which lets one user connect to and view the Desktop of another user's computer, as well as take control of the system's mouse and keyboard to change settings, view system parameters, uninstall and install applications, and attempt repairs.

The idea behind Remote Assistance is to avoid bringing productivity to a screeching halt when a remote user cannot fix a computer related problem, that user can seek help from an expert through Remote Assistance.

Windows Remote Assistance is based on the Remote Desktop Protocol.

Just like this research, Windows Remote Assistance is a remote access technology; however, these two remote access technologies are used for different purposes since Remote Assistance does not run on smartphones. Whereas Windows Remote Assistance cannot give SMS updates on network status, this research will be able to do that. Also, for audit trail purposes, Windows Remote Assistance will not be able to "tell" who logged onto a system previously but this research seeks to overcome that limitation in Windows Remote Assistance.

The ability to control a home appliance in a wireless and remote fashion has provided a great convenience to many people in life. Through a wireless remote controller, people can do remote operations without having direct contact with the appliance itself.

The introduction of the Global System for Mobile communication (GSM) and the use of hand-held mobile phones brought the innovation of distance communication at remote locations. (Chauhan et al., 2011) conducted a research that uses the GSM facility to remotely control systems and appliances such as air conditioners and TVs.

The problem Chauhan and his colleagues addressed in their research was to allow individuals to use their mobile phones to turn off gadgets they would have forgotten to switch off at home while away by just sending SMS to the particular appliance or device. They did this by implementing a microcontroller based control module between the mobile device and appliance to be controlled. The microcontroller then carries out commands from the mobile phone and then communicates the status of a given appliance back to the cellular phone over a GSM network.

SMS based Remote Control System implements a microcontroller –based control module that receives instructions and commands from a cellular phone over a GSM network. The microcontroller then carries out the issued commands and then communicates the status of a given appliance or device back to the cellular phone. This system can even be used to switch on, off or restart some Linux servers, ADSL modems and even printers.

SMS based Remote Control System is a fascinating remote technology application which can be used to monitor the status of household appliances and other gadgets through periodical SMS alerts, just like the application this research seeks to implement which will give regular SMS alerts on the status of a computer network to System Administrators through their mobile phones.

However, this system (SMS based Remote Control System) has nothing to do with remote system administration which makes it quite different from this research which seeks to implement a system for remote system administration purposes. Also, the article on SMS based Remote Control System remained silent about the security of the system unlike this research which is taking security seriously by incorporating self-signed SSL certificate in the android app.

A careful study of the above reviewed works indicates that they have a few similarities and some differences. When it comes to cross-platform, VNC, TeamViewer, LogMeIn and Remote Control System are all cross-platform applications. Also, VNC, TeamViewer and ShowMyPC can be used for collaborative works, presentations and highly interactive meetings.

Smartphones are handheld mobile computers integrated with a mobile telephone feature which usually allow the user to install and run more advanced applications that are also called apps (Yang & Li, 2012).

The major smartphone operating systems in use are Symbian OS, Android OS, Blackberry OS, iOS and Windows Mobile OS of which Android OS is dominant in the mobile market. These operating systems provide platforms for users to develop their own applications that can run on these smartphones.

The researcher tries to explore smartphones technology that can cause an explosion in the way and manner remote system administration is done.

Smartphones are made in such a way that they can be carried with convenience because of their small physical size which makes them excellent for carrying around. Once they are easy to carry and have a built-in keyboard, this research work intends to turn them into tools that can be used to remotely administer computers by the Systems' Administrator.

In effect, this research work seeks to bring some sigh of relief to System Administrators especially those who do not stay in their offices throughout the day because of their busy schedules, but will still like to be hooked up to their computer networks.

2.4 SUMMARY

This chapter looked into some existing remote access technologies and went further to review various remote access systems which are related to the researcher's area of investigation and compares these works with this research work. This chapter, in reviewing related works identifies some limitations of the reviewed works and goes further to state how those limitations will be addressed in this investigation.

CHAPTER THREE

METHODOLOGY

3.1 INTRODUCTION

The chapter also looks at the waterfall model in software development and goes further to justify why the Waterfall model is chosen as the concept the researcher is adopting to develop the smartphone app this research seeks to implement.

Also, the population and sample size for this research is discussed. The questionnaire that will be used to gather the data and analysed is also discussed here. The tools to be used for coding the data and finally for the analysis are also discussed here.

3.2 THE NATURE OF THE RESEARCH

The study will compare remote access technologies and implement a secure smartphone app for remote system administration. The quantitative research method approach which is based on sampling techniques will be used.

The researcher intends to design questionnaires to aid in the data collection process. The raw data collected will then be coded and analysed using SPSS version 17.

3.3 RESEARCH METHOD AND DESIGN

In order for the researcher to be able to implement the android app for remote system administration, the waterfall model was adopted to help in implementing the android app.

The waterfall model is the classical model of software engineering. This model is an activity centred process that prescribes that activities are executed sequentially.

This model consists of five (5) distinct phases and for an activity to start in each phase, the activity or activities in the phase preceding it must finish completely before the next phase can be executed. This model is document intensive and produces at least a document in each of its phases. The phases of the waterfall model are shown in the diagram below.

The diagram in figure 3 below represents the waterfall model.

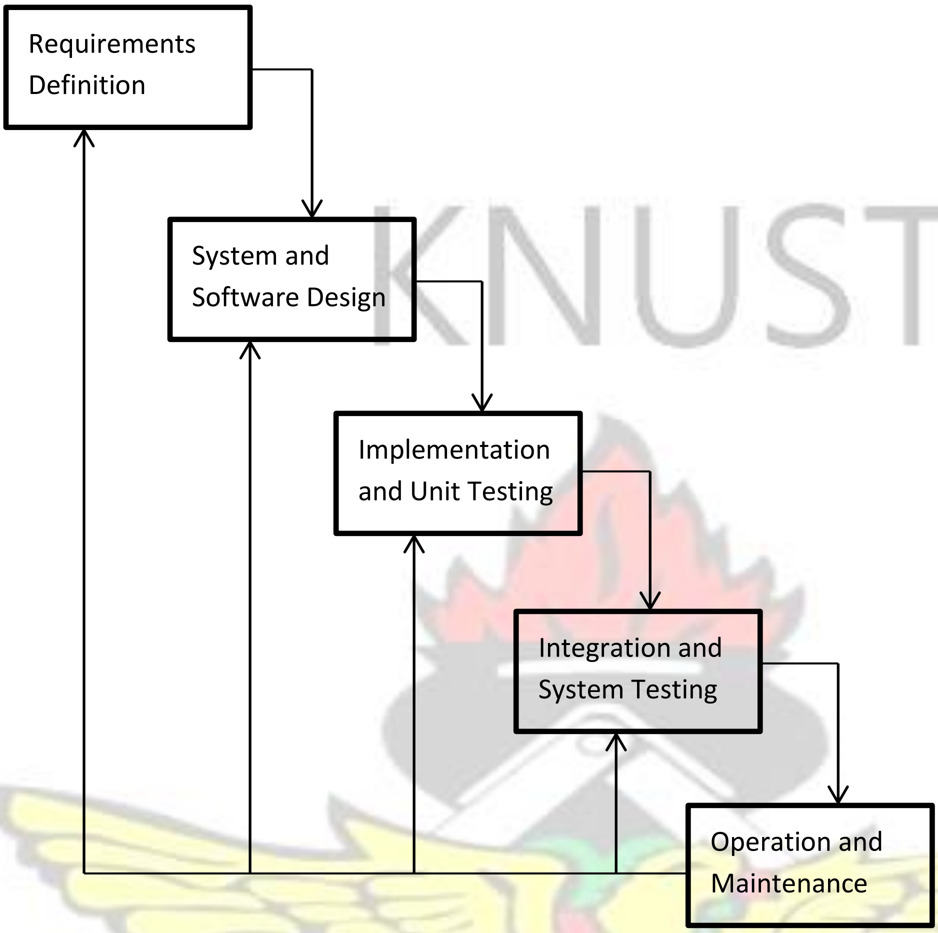

Requirements Definition
System and Software Design
Implementation and Unit Testing
Integration and System Testing
Operation and Maintenance

Figure 3: The Waterfall Model (Munassar & Govardhan, 2010)

The researcher has adopted the water fall model as the preferred methodology in developing the android app because of its several advantages in using it to develop a system.

This model is instructive because it emphasizes the important stages of the project development and it is also very easy to understand and implement.

As the model emphasizes planning at the early stages, it ensures design flaws are dealt with before they develop (Munassar & Govardhan, 2010).

One other formidable reason why the waterfall model was adopted is because it reinforces good habits, that is define-before-design and design-before-code. It identifies deliverables and milestones during development.

The model further produces several important documents such as User Requirement Document (URD) and Software Requirement Document (SRD) which are very important documents in any software development process.

Despite its several advantages, one major disadvantage of the waterfall model is that because the actual development of the system comes late in the process, one does not see results for a long time. This delay can be disconcerting to customers and management. However, once this is purely for research work and does not concern any customer or management, the above limitation or disadvantage of this model is of little or no concern here.

3.3.1 POPULATION AND SAMPLE

A research problem relates to a specific population and this population usually involves the total collection of all units of analysis about such a population which the researcher wishes to make explicit conclusions (Naidoo, 2011).

Since it is expensive and impractical to involve all members of the targeted population in a research study, researchers in all cases mostly rely on data obtained from a sample (part) of the population.

The targeted population will be Network Administrators, System Administrators, Computer Technicians and related computer users who have considerable knowledge in computers in one way or the other and also have the necessary knowledge about remote access protocols and software. Due to the fact that the targeted population are rare to find, the researcher intends to get responses from a minimum of fifty (50) respondents. Questionnaires will be designed and administered in Tamale in the Northern Region and Accra in the Greater Accra Region respectively in order to obtain the minimum of 50 respondents.

3.3.2 QUESTIONNAIRE DESIGN

The strength of data analysis depends on the quality of data which by extension depends on good design of the data collection instrument, that is the questionnaire and of the data collection procedures (Burgess, 2001).

In designing the questionnaire to gather data about remote technologies and remote access software, the researcher started with an introduction to assure respondents their responses will be used strictly for academic purposes while ensuring confidentiality of respondents.

The questionnaire further gave instructions on how to give responses in order to limit respondents' errors.

The following is a comprehensive breakdown of the types of questions that were presented to the respondents:

Questions 1 to 3 seeks to take the personal details of respondents.

Question 4 seeks to know whether respondents have ever used remote access software.

Question 5 seeks to know the current usage of remote access technologies by system administrators.

Question 6 seeks to know how long respondents have been using remote access software.

Question 7 seeks to find out whether respondents have knowledge about remote access protocols or technologies.

Question 8 seeks to find out which remote access protocol or technology respondents have knowledge about.

Question 9 seeks to find how informed respondents are about the choice they made in question 7.

Question 10 seeks to find out which remote access software respondents have used before.

Question 11 seeks to find out what inspires respondents to continually use their choice of remote access software.

Question 12 seeks to find out whether respondents know the protocol or technology their choice of remote access software in question 9 is based on.

Question 13 seeks to find out from respondents which protocol their choice of remote access software in question 9 is based on.

Question 14 seeks to allow respondents to rate their choice of remote access software based on efficiency with regards to the remote access technology that software is based on.

Question 15 seeks to allow respondents to rate their choice of remote access software based on reliability with regards to the remote access technology that software is based on.

Question 16 seeks to allow respondents to rate their choice of remote access software based on performance with regards to the remote access technology that software is based on.

Question 17 seeks to find out from respondents whether their choice of remote access software is user friendly.

Question 18 seeks to find out whether respondents will like to see new features added to their choice of remote access software in question 9.

Question 19 seeks to find out which remote access software respondents will like to see new features added to.

Question 20 seeks to allow respondents to present the new features they will like to see added to their choice of remote access software in question 18.

Question 21 seeks to find out from respondents whether innovations are relevant in respondents' industry.

Question 22 seeks to find whether respondents are ready to accept IT innovations.

Question 23 seeks to find out whether respondents are ready to and accept and use a remote system administration application that runs on a smartphone.

Question 24 seeks to find out the reasons why users will accept a remote system administration application that runs on a smartphone.

Also, in under taken the performance test of the RDP protocol, the RFB protocol and the secure android app, another questionnaire was designed and its breakdown is as follows:

Question 1 seeks to allow respondents rate the performance of the RDP protocol, RFB protocol and the secure android app based on their response times.

Question 2 seeks to allow respondents' rate the availability of the above protocols and the secure android app.

Both questionnaires ended with a plea to respondents to feel free to add anything they may deem necessary but which was not captured in the questions.

Both questionnaires are shown in the appendices.

The above questions were important and of great significance to this study as they assisted the researcher in gathering vital information about remote access protocols or technologies and remote access software.

3.3.3 DATA ANALYSIS

In trying to make meaning out of the raw data gathered from respondents through the questionnaire, the researcher must analyse the said collected data. The raw data collected from the survey will be changed into a structure that will be suitable for analysis through the process of coding.

Every response item on the questionnaire needs to be entered as a number code (except narrative text). To do this, numbers are assigned to respondents responses prior to data entry. This process is called data coding.

After this coding process, SPSS will be used to analyse the data and draw appropriate diagrams that will reveal interesting trends between collected data.

3.3.4 REQUIREMENTS DEFINITION OR SPECIFICATION

The requirements definition is specify the requirements of the system. The system to be developed consists of two components which are an android app and a PHP application which will be used by only network administrators for remote system administration purposes.

Network administrators find it very difficult if not impossible to monitor their networks once they (Administrators) are out of their stations or offices.

The system is supposed to monitor the network and report the network status such as whether the link is down or up to network administrators through their android smartphones using SMS.

The app when implemented is also supposed to allow network administrators' login to servers that will run a PHP application and be able to create users or add users to the network using their android smartphones which will run the android application.

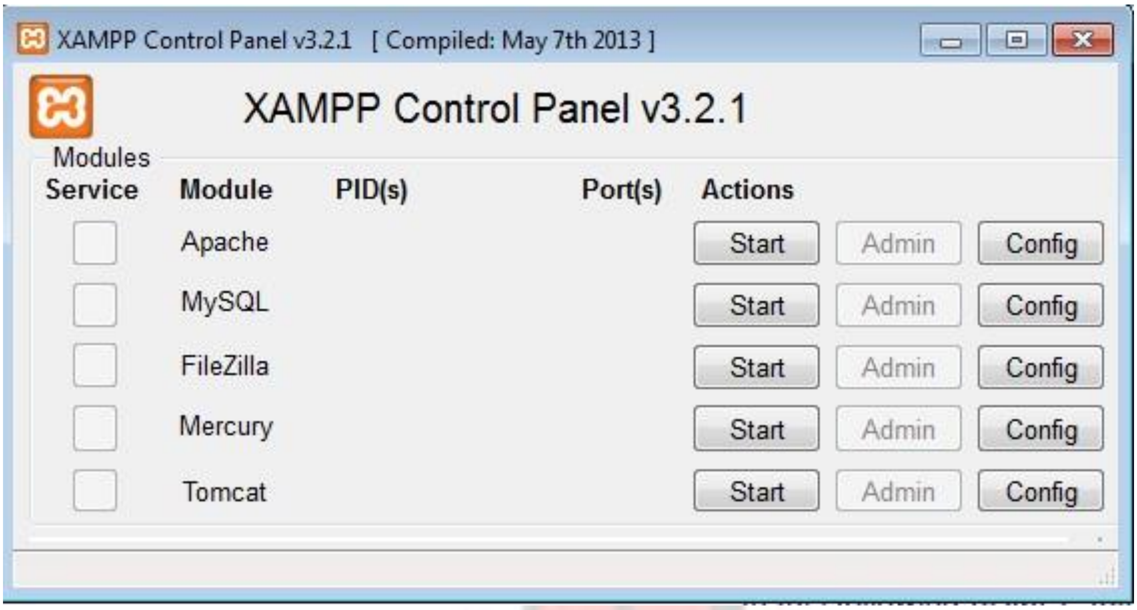
Using this system, network administrators will also be able to create and view text files on servers using their android smartphones while away from the servers.

Finally, network administrators will be able to shut down or even restart their servers remotely from their smartphones.

The PHP component of the system needs a minimum of Windows XP platform but the researcher recommends at least Windows Server 2003 Operating System for maximum efficiency. Also, the PHP component of the system also needs XAMPP application to be installed on the remote computer (Server) before it can work.

When the XAMPP application is installed, in its installation directory, there is an htdocs folder; the PHP files stored in a folder must be copied into this htdocs folder located in the XAMPP installation directory. After this, the user (Network Administrator) only needs to run this XAMPP application on the server to be monitored.

XAMPP is a small and light Apache distribution containing the most common web development technologies in a single package (Dvorski, 2007).
XAMPP(**X** read as cross-platform, Apache HTTP Server, MySQL, PHP and Perl) is free and open source cross-platform web server solution stack package consisting mainly of Apache HTTP Server, MySQL database, and interpreters for scripts written in PHP and Perl programming languages. The choice of XAMPP is suitable because it is a whole package that comes with almost all the tools the researcher intends to use to build the system. XAMPP can be downloaded from http://www.apachefriends.org/en/**xampp**-windows.html. This is to avoid installing each individual application separately. The interface of XAMPP is as shown in figure 4 below.



XAMPP Control Panel v3.2.1 [Compiled: May 7th 2013]

XAMPP Control Panel v3.2.1

Modules

Service	Module	PID(s)	Port(s)	Actions		
□	Apache			Start	Admin	Config
□	MySQL			Start	Admin	Config
□	FileZilla			Start	Admin	Config
□	Mercury			Start	Admin	Config
□	Tomcat			Start	Admin	Config

Figure 4: XAMPP (2015)

For best performance, XAMPP needs a minimum of 2GB of RAM, a minimum of 1.5GB free hard disk space and 2GHz CPU speed.

3.3.5 CONSTRAINTS

The system will only work when there is internet service.

3.3.6 NON-FUNCTIONAL REQUIREMENTS

The system shall ensure that unauthorized users do not have access to it since access permissions can only be changed by the network administrator.

In terms of, performance, the system will react very quickly to user inputs and will also be very accessible to users since it will be web-based (users only need to have access to internet to access it).

The system will also be user friendly because the graphical user interface will be wellformed and informative error messages will be incorporated into the system.

3.3.7 SYSTEM AND SOFTWARE DESIGN

In this phase, the sub-systems and or components that must be put together to come up with the complete system and the interconnections between these sub-systems are identified. Also, how the system interacts with other systems and users is identified here.

The architecture of the system is as shown in figure 5 below.

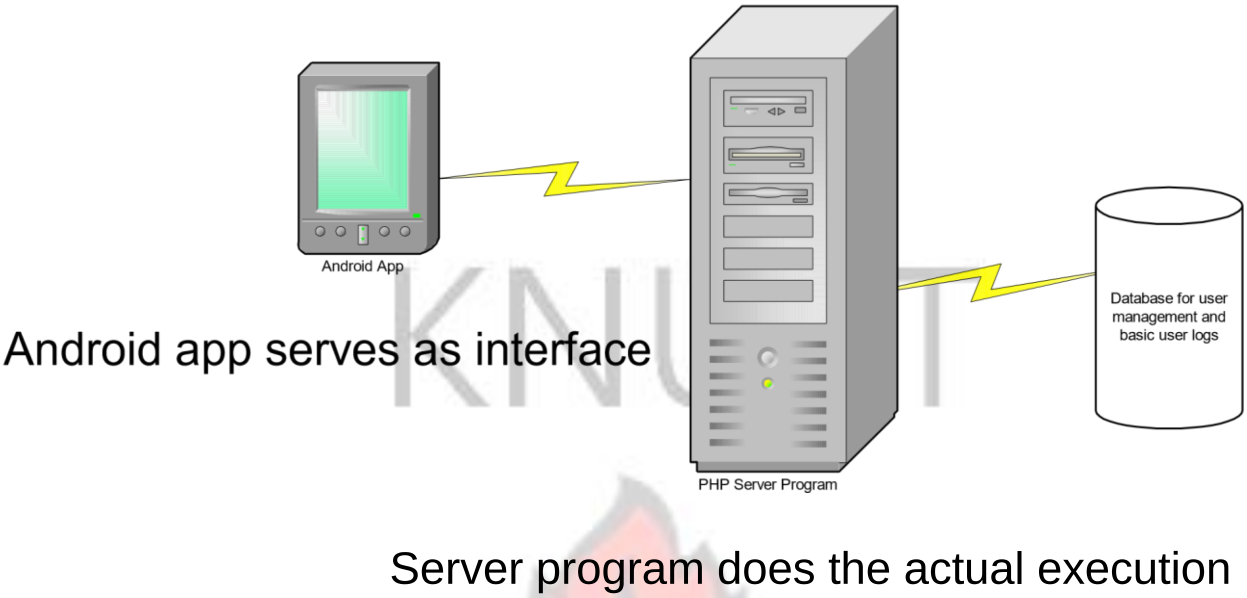

Android App
Android app serves as interface
PHP Server Program
Database for user management and basic user logs
Server program does the actual execution

Figure 5: System's Architecture. Source: Author's Construct

In this architecture, the sub-systems that are needed to make up the complete system are the android app, the PHP application and the database.

The android app will run on an android smartphone and will be responsible for issuing commands to the remote server. In effect the android app will be like an interface to the server. The PHP application will run on the server machine which will actually be responsible for processing and returning all requests from the android app. The database will keep track of all administrators who logon to the system and the activity performed using their smartphones for audit trail purposes.

3.3.8 DEVELOPMENT TOOLS AND TECHNOLOGIES

In developing this system, some tools and technologies will be used to aid the researcher come up with a system that will meet its intended objectives.

The system will be built based on the Virtual Network Computing (VNC) technology which is otherwise called Remote Frame Buffer (RFB) protocol. This technology was discussed earlier in the preceding chapter.

The tools that will be used in developing the system are outlined in table 1 below.

Table 1: Tools used in developing the system

Tool	Purpose
Eclipse IDE	Programming language for developing android application
PHP	Scripting language for developing PHP application that will run on a server machine
MySQL	DBMS for designing and keeping track of users who logon to server using android phone
Microsoft Office 2010	For writing documentation

Source: Author's construct, 2014

3.3.9 THE PROPOSED SECURE RFB PROTOCOL AND IMPLEMENTATION OF AN ANDRIOD SMARTPHONE APP FOR REMOTE SYSTEM ADMINISTRATION

Security will be incorporated on top of the RFB protocol the android app is based on. This is to make it secure based on the fact that this RFB protocol has some security lapses as discussed in the literature review.

The researcher intends incorporating Secure Socket Layer (SSL) security into the android app through self-signed SSL certificate so that secure encrypted connections can be established between the client (smartphone) and the server. This is to guard against Man-In-The-Middle (MITM) attacks.

This self-signed SSL will be incorporated using "bcprov-jdk150on-146.jar" class to create a Keytore and saved in "C:\androidproject". The above file which is a java class can be downloaded from www.bouncycastle.org/download/ bcprov-jdk150on-146.jar. Then a keytool will be used to generate a key. This generated key will then be exported from the ".keystore file" to ".cer file" using the command "-export –alias androidprojects –keystore C:\androidproject\androidprojectsslcert –cer".

A class called "MyAndroidClient" will then be written to implement this self-signed SSL certificate that will be created. The idea here is to do certificate pinning with the self-signed SSL certificate created on the server the android app will be communicating with so as to provide end-to-end security against Man-In-The-Middle (MITM) attack.

(Entrust Incorporation, 2007) defined a digital certificate as an electronic file that is used to identify people and resources over a network such as the internet. Certificates are issued by Certificate Authorities (CAs); however, individuals can issue their own certificates which are referred to as self-signed certificates. The role of the certificate issuer is to validate the certificate holder's identity and to make sure the certificate is signed so that it cannot be tampered with by other people.

Secure Socket Layer (SSL) is a cryptographic protocol that creates an encrypted communication channel between a server and client that makes internet traffic indecipherable to third parties that might intercept them (Roosa & Schultze, 2010). This secure connection is established using SSL digital certificate and public encryption key.

The main purpose of SSL is to provide end-to-end security against Man-In-The-Middle (MITM) attacks (Georgiev et al., 2012).

A self-signed certificate, according to (Code Project, 2014) is a certificate signed by the individual who created it rather than a trusted Certificate Authority (CA). This research intends using a self-signed certificate because they are free to use, they are also very convenient in mobile development since mobile apps in most cases interact with only one server unlike web browsers. Also, self-signed certificates work like certificates from a CA if well implemented.

According to (Mathew & Jacob, 2008) SSL protocol is now universally accepted in the World Wide Web for authentication and encrypted communication between clients and servers.

This is how SSL works, before a secure link can be established between a server and a client, the client will first of all send a 'Client Hello' message to the server, indicating that a secure session is requested, the server then responds by sending the client its server certificate which includes its public key.

The client will then verify that the server's certificate is valid and has been signed by a CA, whose certificate will be in the client's database and also verify that this certificate is not expired. Once the certificate is authenticated, the client then generates a one-time unique session key and encrypts it with the server's public key. Then the client sends the encrypted session key to the server so that they will both have copies. The server then decrypts the message using its private key and recovers the session. After this, a secure communication link will then be established between the server and client where both server and client can use the session key to send encrypted information back and forth (Entrust Incorporation, 2007).

3.3.10 EVALUATING THE PERFORMANCE OF THE RDP, RFB, AND THE PROPOSED SECURE RFB PROTOCOL

Software testing is very critical in ensuring software quality and represents the ultimate review of software specification, design and coding (Ahamed, 2009).

The researcher intends to look at the performance of the RFB protocol, the RDP protocol and the android app this research seeks to implement which is based on a Secure RFB protocol (SRFB) with self-signed SSL certificate on top of the RFB protocol.

In undertaken this performance test, the researcher intends pinging a server connected to a client through remote desktop (RDP protocol) in order to get its response time. A ping results will also be obtained from a server connected to a client through VNC (RFB protocol) and another ping results will be obtained from a server connected to a smartphone through the android app this research seeks to implement which is based on a secure RFB protocol so that the obtained response times can be compared. However, to be able to ping from an android smartphone, the researcher intends downloading and installing Terminal Emulator for android.

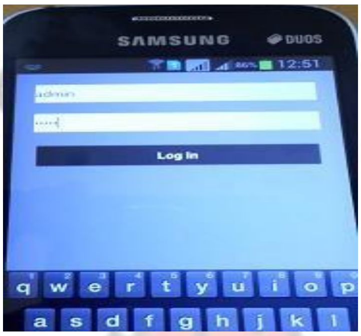
The screen shots from the pinged results will then be presented.

Nine (9) administrators will also be engaged to use the Remote Desktop (RD) which is based on the RDP protocol, use VNC which is based on the RFB protocol and the android app which is based on a Secure RFB (SRFB) protocol and thereafter through a questionnaire rate the individual performance of the remote software in terms of their response times and availability.

These responses from the nine administrators will be presented in a table and a bar chart.

3.3.11 USER INTERFACE DESIGN

When the android app is run, the first screen that displays is as shown in figure 6 below. Before a user (Network Administrator) can have access to the application, that user must enter a valid username and a password in order for access to be granted.



admin

Figure 6: Login Screen of Android App. Source: Author's Construct 2014

Upon successful login, in order for the network administrator to be able to administrator or monitor any server using the android app (android phone), the administrator must first of all add the server to the list of servers to be monitored through the android application. This is done by entering the Server's Name, IP Address, Port number and clicking the Save button.

The screen shown in figure 7 below is what the network administrator will use to add a server in order to be able to monitor it.

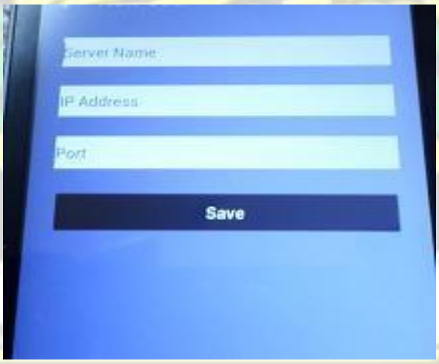


Figure 7: Interface for adding servers. Source: Author's Construct 2014

3.3.12 DATABASE

In order for the system to be able to keep track of network administrators who logon to the system and also keep track of the users created by administrators through their android phones, a database is required. The system also needs a database to keep track of servers added onto the system by network administrators, and again a database is needed to accomplish this.

The diagram shown in figure 8 below represents the Entity Relational (ER) diagram.

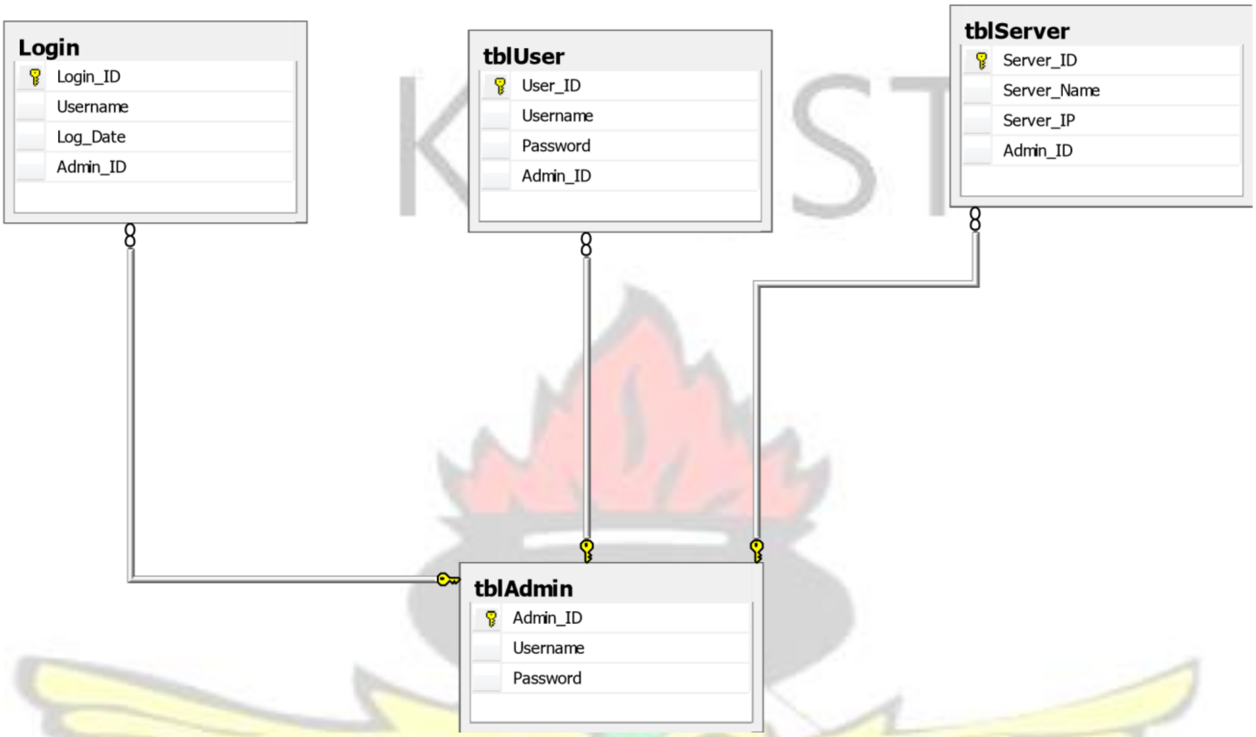


Figure 8: Entity Relational Diagram. Source: Author's Construct 2014

3.3.13 USE CASE DIAGRAM

The use case model uses actors and use cases.

Use case concepts are simply an aid to defining what exists outside the system which are referred to as actors and what should be performed by the system referred to as cases (Wegmann and Genilloud, 2000).

The diagram shown in figure 9 below shows the use case diagram.

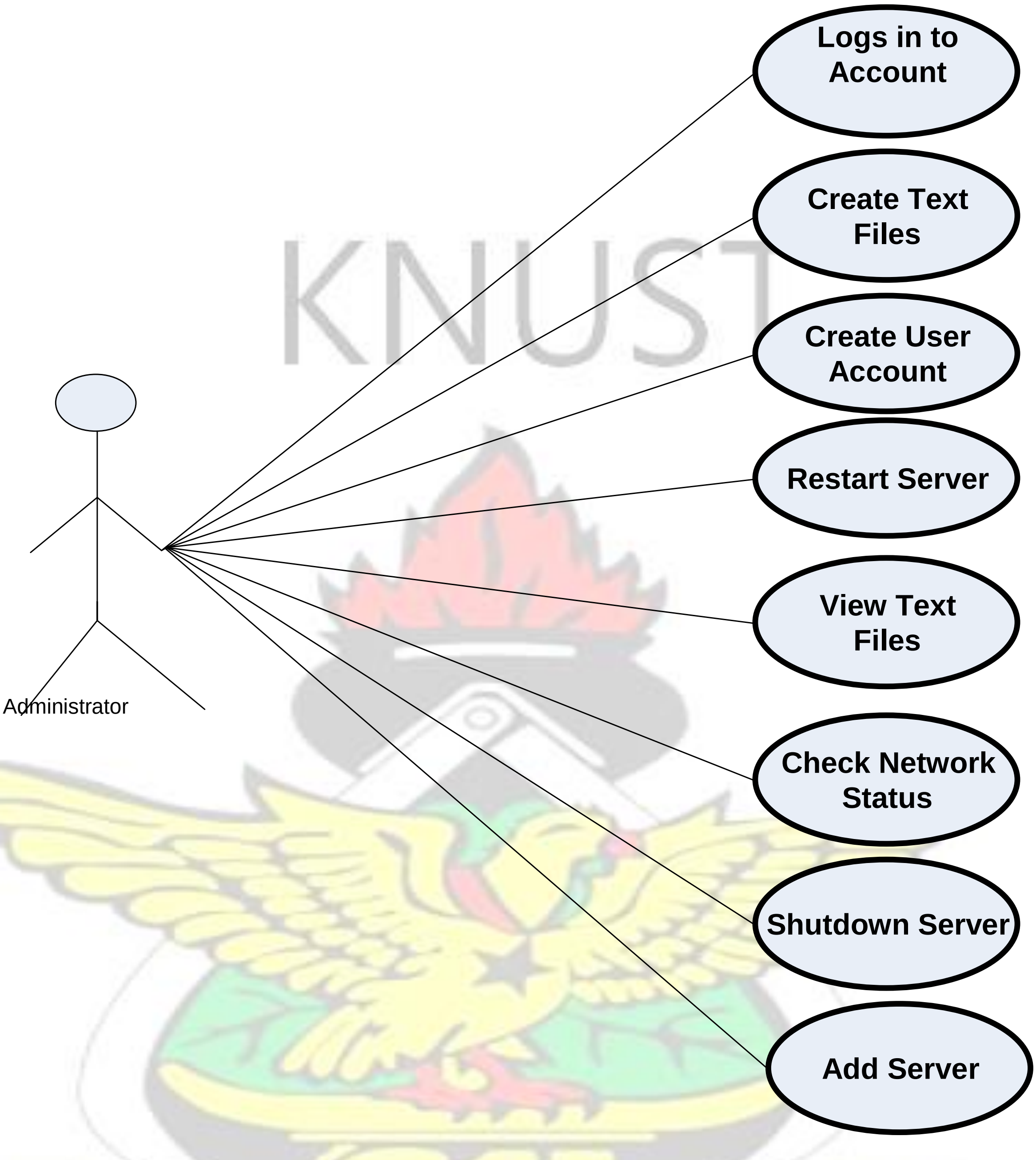


Figure 9: Use Case Diagram. Author's Construct, 2014

Table 2: Use Case Descriptions

ACTOR	ACTIVITY
Administrator	✓ Logs in to administrator account using smartphone ✓ Create text files through smartphone ✓ Create users using smartphone ✓ Restart server using smartphone ✓ View and modify text files ✓ Check network status through SMS ✓ Shutdown server using smartphone ✓ Add server in order to be able to monitor or administer it

Source: Author's construct

3.4 ACTIVITY DIAGRAM

An activity diagram shows the activities involved in a process.

The diagram in figure 10 below shows an activity diagram for creating a user.

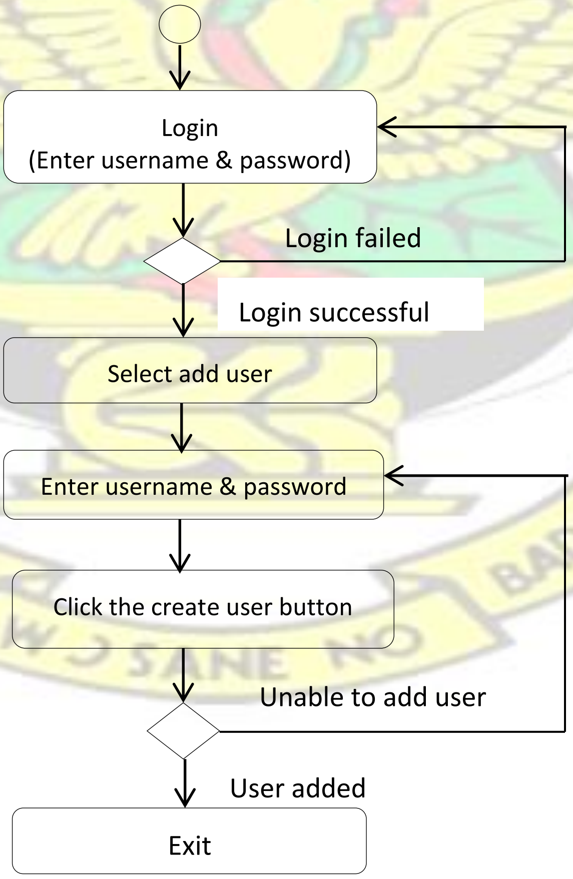

Login
(Enter username & password)
Login failed
Login successful
Select add user
Enter username & password
Click the create user button
Unable to add user
User added
Exit

Figure 10: Activity diagram. Author's Construct 2015

3.5 SEQUENCE DIAGRAM

A sequence diagram shows interactions between actors and the system and also between system components (Sommerville, 2009).

The diagram in figure 11 below is a sequence diagram of the system.

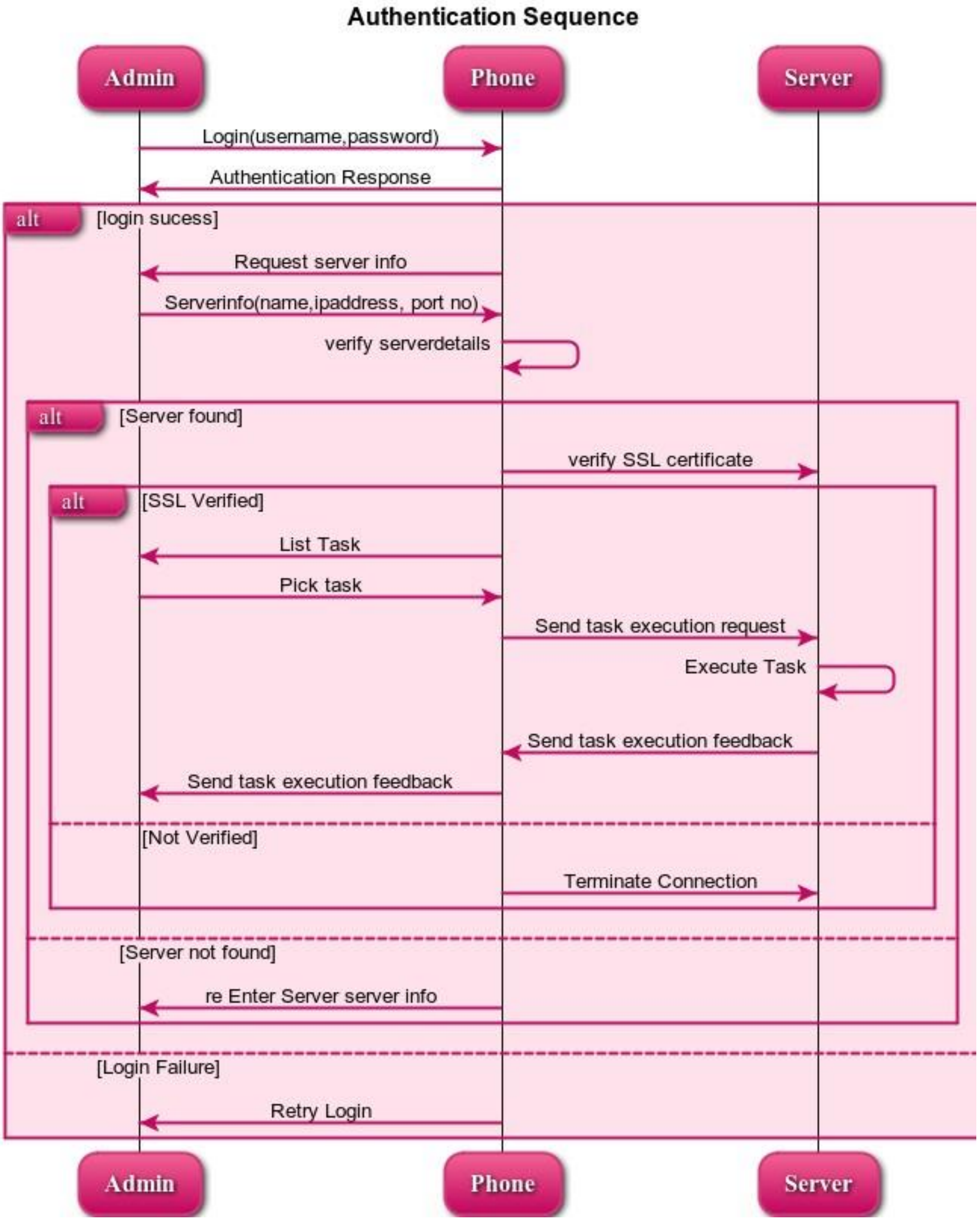


Figure 11: Sequence diagram of system. Source: Author's construct 2015

3.6 SUMMARY

The chapter looks at the software requirements and also went further to look at the database relationship diagram. Snapshots of the system’s interface are also included here.

The tools that will be used to develop the system were also discussed here.

How security (self-signed SSL certificate) will be incorporated into the android app is also presented in this chapter.

The constraints of the system were also looked at here. Use case diagrams are also discussed in this chapter.

How the researcher intends to carry out a performance test of the RDP protocol, the RFB protocol and the secure android app are all presented in this chapter.

CHAPTER FOUR

DATA ANALYSIS, IMPLEMENTATION, CODING AND PERFORMANCE TEST

4.1 INTRODUCTION

This chapter presents the research findings of the study. The methodology explained earlier in chapter three (3) is used to evaluate responses from respondents.

The analyses of the administered questionnaires are done through tables and graphs and findings from the analysis are then compared with reviewed literature.

Also, how self-signed Secure Socket Layer (SSL) certificate was incorporated into the system to make secure connection established between the client and the server is also outlined in this chapter.

Performance test of the RFB protocol, RDP protocol and the android app is also carried out in this chapter.

In this chapter, the researcher also presents the pseudo codes of some of the implemented system's functionality and the screen shots of the implemented application. The screen shots shown were generated when the researcher was testing the system (smartphone app).

4.2 DATA ANALYSIS

The total number of respondents who responded to this survey were sixty seven (67).

Through the analysis of this data, interesting trends are revealed which are presented through the research findings presented below:

4.2.1 GENDER

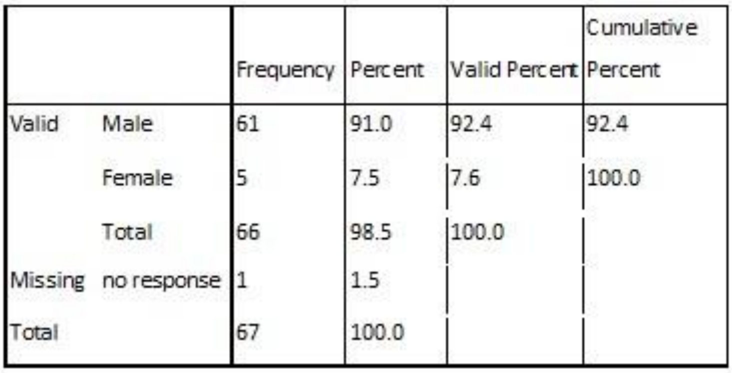
In this study, 61 of the respondents, representing 91.0 % of the respondents were males, 5 of the respondents, representing 7.5 % of the respondents were females and only 1 of the respondent which represents 1.5 % of the respondents did not specify the gender on the questionnaire. Looking at the table below, the valid percentage of male respondents is

92.4% representing 61 male respondents and that of the females is 7.6% representing 5 female respondents.

From the research, it can be deduced that more males are into the information technology industry than females.

Table 3 below provides information about the gender of respondents.

Table 3: Gender of respondent



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	61	91.0	92.4	92.4
	Female	5	7.5	7.6	100.0
	Total	66	98.5	100.0	
Missing	no response	1	1.5		
Total		67	100.0		

Source: Field Survey, 2014

The bar chart shown below in figure 12 represents the gender of respondents.

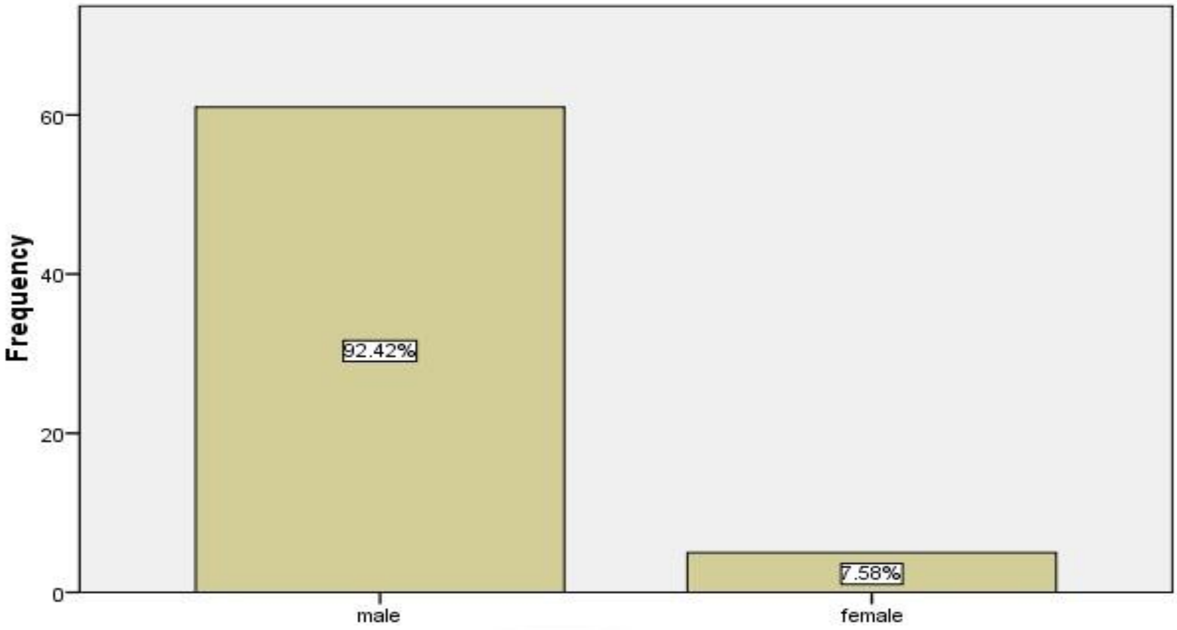


Figure 12: Gender of respondent. Source: Field Survey 2014

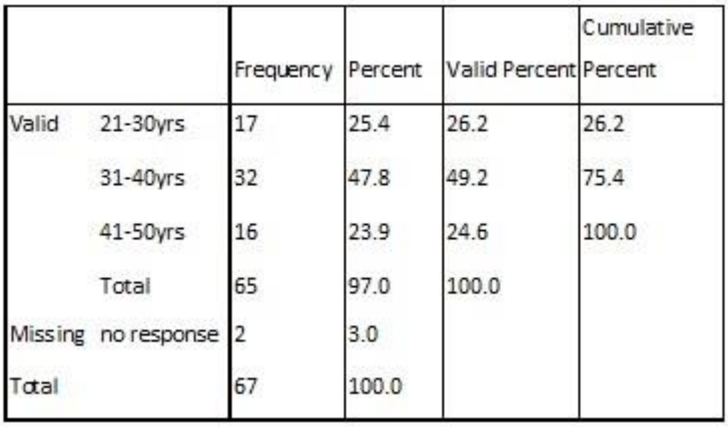
4.2.2 AGE OF RESPONDENT

As presented in table 4 below, the ages of 17 of the respondents is between 21-30yrs representing, 25.4 % of the respondents, the ages of 32 of the respondents is between 3140yrs, representing 47.8 % of the respondents, the ages of 16 of the respondents is between 41-50yrs, representing 23.9 % of the respondents and 2 respondents, representing 3.0 % of the respondents did not indicate their ages on the questionnaire.

The valid percentage of respondents aged between 21-30yrs is 26.2 %, that of 31-40yrs is 49.2 and that of 41-50yrs is 24.6%.

It is clear from the research that, people above the ages of 50yrs are very scarce in the information technology industry, whilst people aged between 21-40yrs are dominant in this industry.

Table 4: Age of respondent



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	21-30yrs	17	25.4	26.2	26.2
	31-40yrs	32	47.8	49.2	75.4
	41-50yrs	16	23.9	24.6	100.0
	Total	65	97.0	100.0	
Missing	no response	2	3.0		
Total		67	100.0		

:

Source: Field Survey, 2014

The bar chart shown in figure 13 represents the age of respondents.

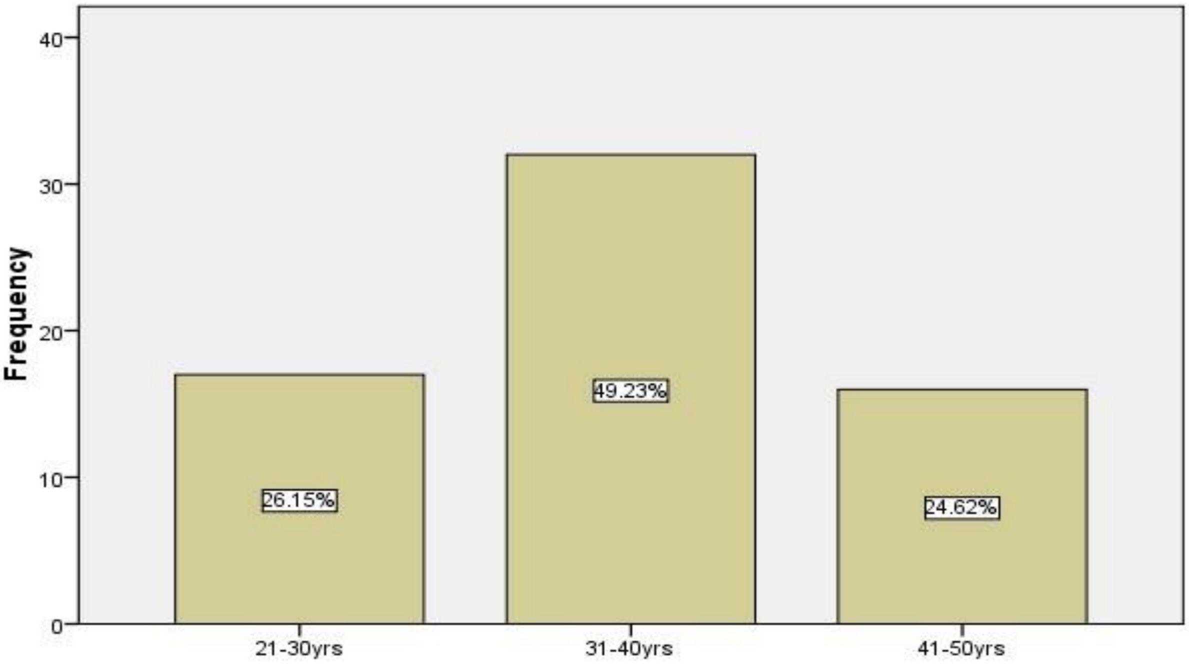


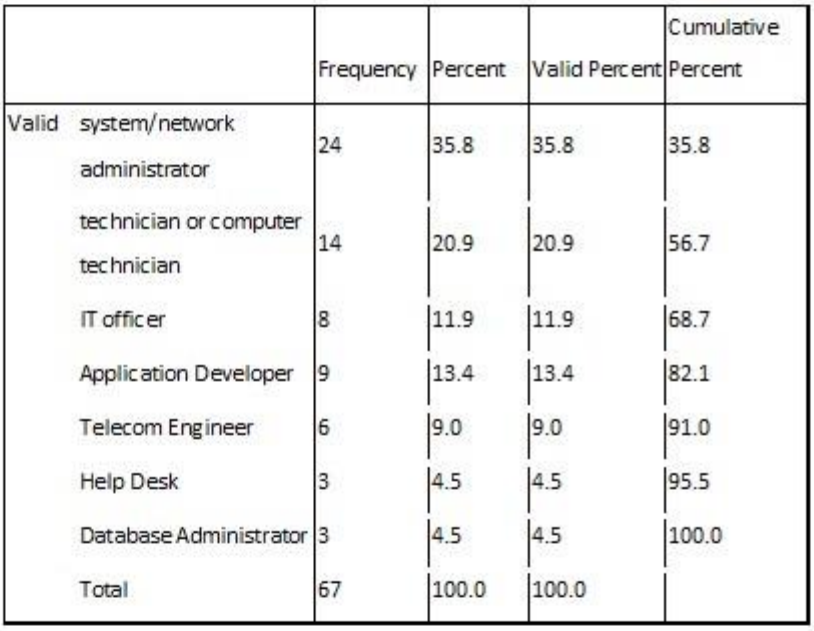
Figure 13: Age of respondent: Source: Field Survey, 2014

4.2.3 OCCUPATION OF RESPONDENT

As shown in table 5 below, 24 of the respondents which represent 35.8 % of the respondents are system/network administrators, 14 of the respondents which represent 20.9 % of the respondents are computer technicians, 8 of the respondents representing 11.9 % of the respondents are IT Officers, 9 of the respondents representing 13.9 % of the respondents are Application developers, 6 of the respondents representing 9.0 % of the respondents are Telecom Engineers, 3 of the respondents representing 4.5 % of the respondents are Help Desk personnel and 3 of the respondents also represent 4.5 % of the respondents are Database Administrators.

From the study, the most common job title among the respondents is System Administrator with Help Desk and Database Administrators being the least common ones.

Table 5: Occupation of respondent



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	system/network administrator	24	35.8	35.8	35.8
	technician or computer technician	14	20.9	20.9	56.7
	IT officer	8	11.9	11.9	68.7
	Application Developer	9	13.4	13.4	82.1
	Telecom Engineer	6	9.0	9.0	91.0
	Help Desk	3	4.5	4.5	95.5
	Database Administrator	3	4.5	4.5	100.0
	Total	67	100.0	100.0	

Source: Field Survey, 2014

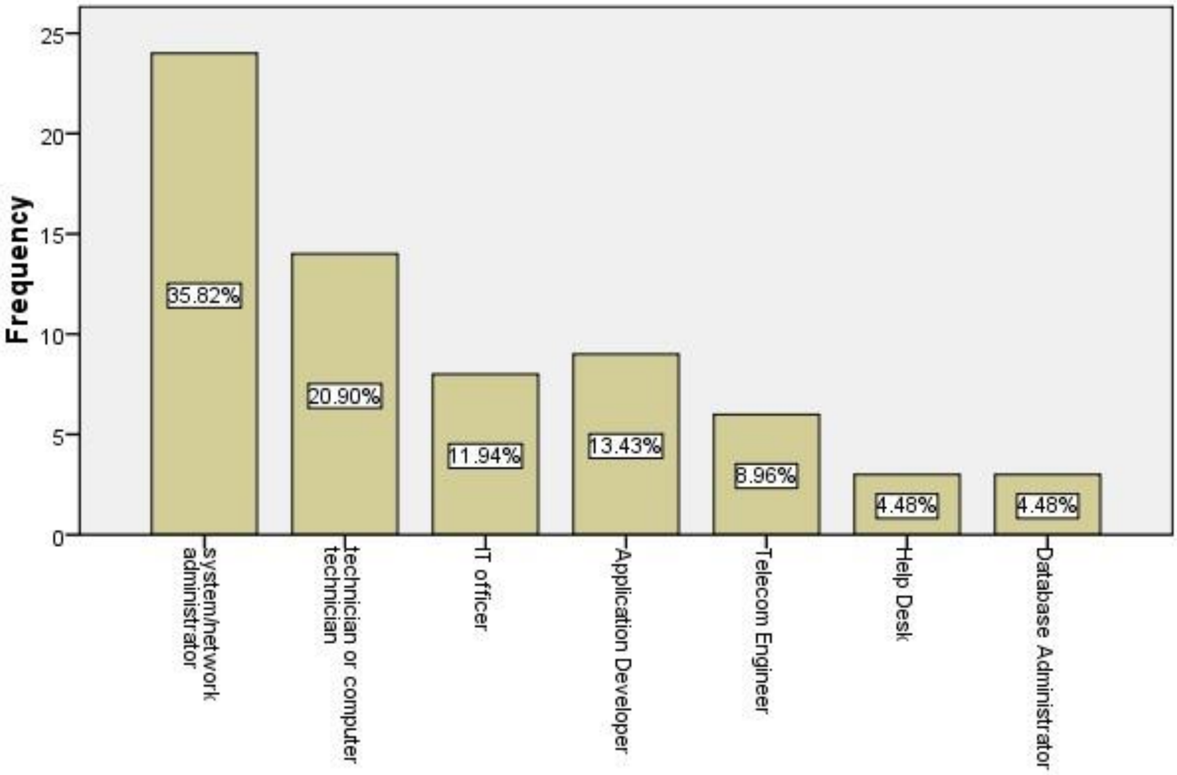


Figure 14: Occupation of respondent. Source: Field Survey 2014

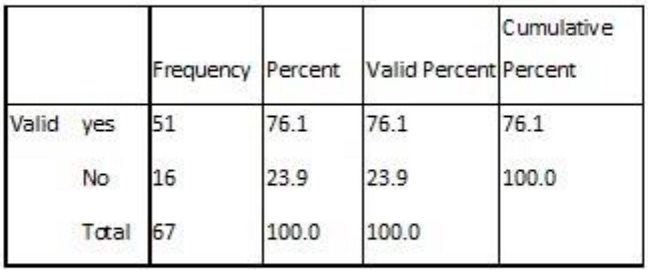
4.2.4 RESPONDENT EVER USED REMOTE ACCESS SOFTWARE?

From table 6 shown below, 51 of the respondents representing 76.1 % of the respondents have ever used remote access software in carrying out their duties and 16 of the respondents representing 23.9 % of the respondents have never used remote access software in carrying out their duties.

From the findings, it can be seen that majority of people in the information technology industry are aware of and have actually used remote access software.

The bar chart shown in figure 15 represents respondents who have ever used and those who have never used remote access software.

Table 6: Respondent ever used remote access software



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	51	76.1	76.1	76.1
	No	16	23.9	23.9	100.0
	Total	67	100.0	100.0	

Source: Field Survey, 2014

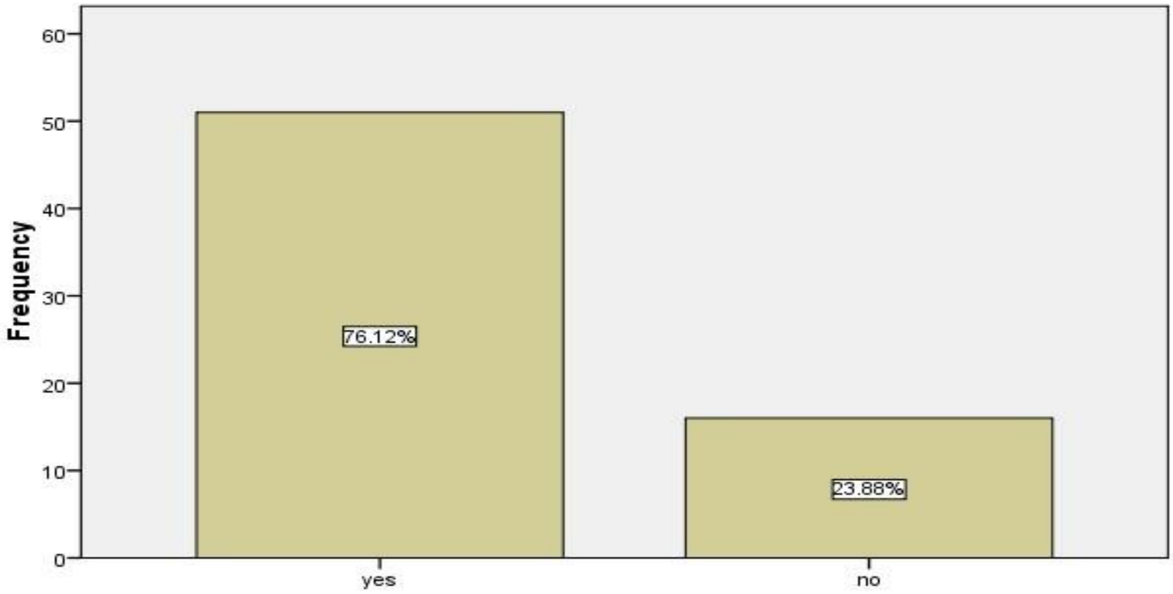


Figure 15: Respondent ever used remote access software. Source: Field Survey 2014

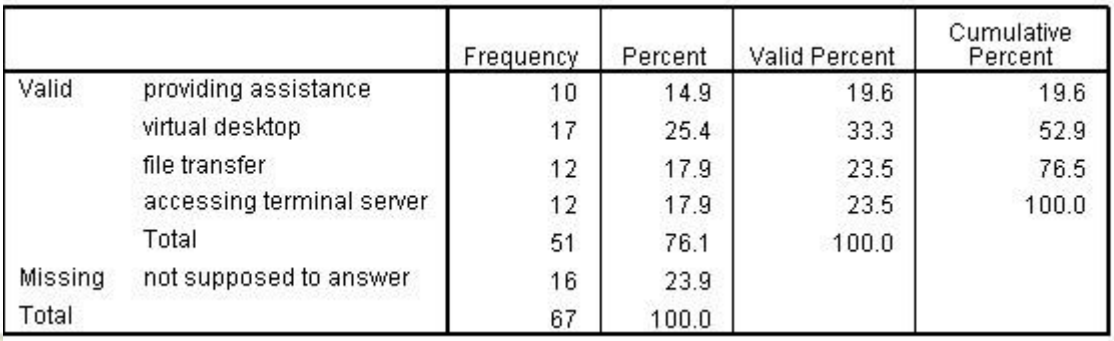
4.2.5 CURRENT USAGE OF REMOTE ACCESS SOFTWARE

From table 7 shown below, 51 of the respondents representing 76.1 % of the respondents indicated what they usually use remote access software to do in their line of duties and 16 of the respondents representing 23.9 % of the respondents have never used remote access software in carrying out their duties.

From the findings, 10 of the respondents, representing 19.6 % of the valid responses use remote access software for providing assistance, 17 of the respondents, representing 33.3% of the valid responses use remote access software for virtual desktop, 12 of the respondents, representing 23.5 % of the valid responses use remote access software for file transfer and the remaining 12 responses, representing 23.5 % of the valid responses use remote access software for accessing terminal servers.

The bar chart shown in figure 16 represents the duration the current usage of remote access software by network administrators.

Table 7: Current usage of remote access software



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	providing assistance	10	14.9	19.6	19.6
	virtual desktop	17	25.4	33.3	52.9
	file transfer	12	17.9	23.5	76.5
	accessing terminal server	12	17.9	23.5	100.0
	Total	51	76.1	100.0	
Missing	not supposed to answer	16	23.9		
Total		67	100.0		

Source: Field Survey, 2014

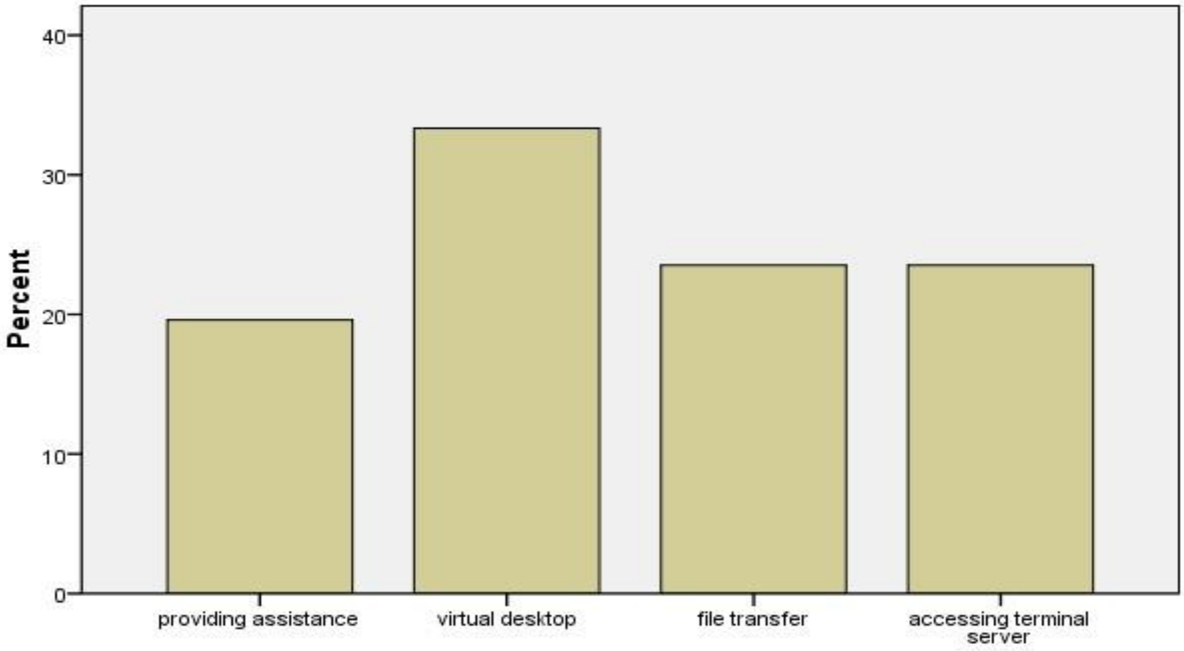


Figure 16: Current usage of remote access software. Source: Field Survey 2014

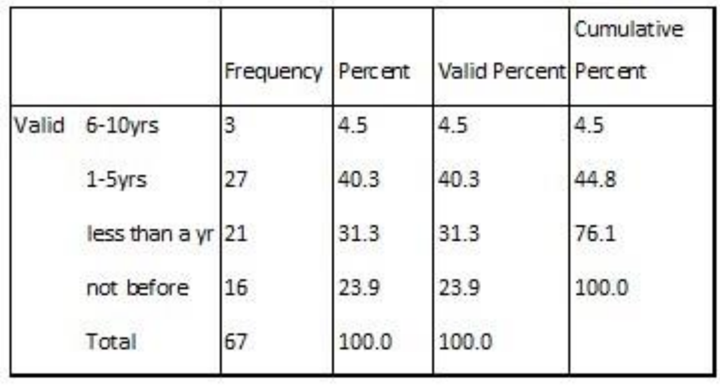
4.2.6 DURATION RESPONDENT HAS BEEN USING REMOTE SOFTWARE

As shown in table 8, 3 of the respondents representing 4.5 % of the respondents have been using remote access software for 6-10yrs, 27 of the respondents representing 40.3% of the respondents have been using remote access software for 1-5yrs, 21 of the respondents representing 31.3 % of the respondents have been using remote access software for less than a year and 16 of the respondents representing 23.9 % have never used remote access software in their line of duty before.

From the findings, majority of respondents have been using remote access software for 1-5yrs.

The bar chart shown in figure 17 represents the duration respondents have been using remote access software.

Table 8: Duration respondent has been using remote software



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	6-10yrs	3	4.5	4.5	4.5
	1-5yrs	27	40.3	40.3	44.8
	less than a yr	21	31.3	31.3	76.1
	not before	16	23.9	23.9	100.0
	Total	67	100.0	100.0	

Source: Field Survey, 2014

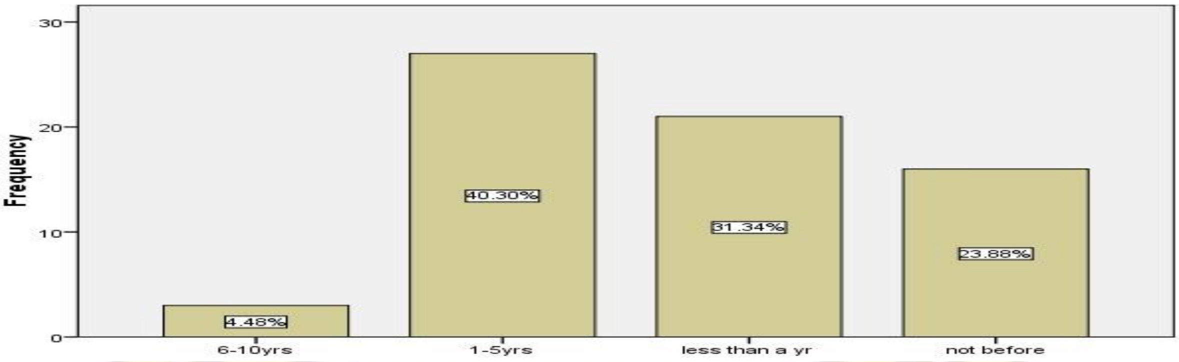


Figure 17: Duration respondent has been using remote access software. Source: Field Survey 2014

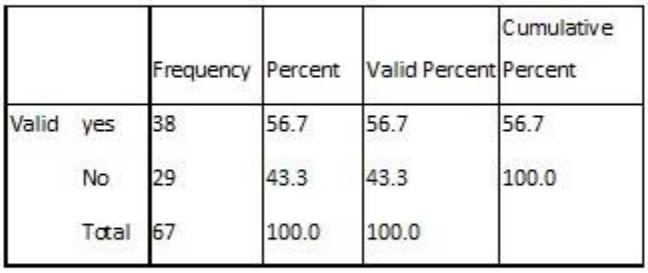
4.2.7 RESPONDENT'S KNOWLEDGE ABOUT THE PROTOCOLS/TECHNOLOGIES

As shown in table 9, 38 of the respondents representing 56.7 % of the respondents have knowledge about the protocols or technologies used in developing remote access software and 29 of the respondents representing 43.3% of the respondents have no knowledge of the protocols used in developing remote access software.

From the study, though majority of the respondents have knowledge about the protocols used in building remote access software, the difference between those who have knowledge and those who do not have knowledge about these protocols is very close and so software users who are technical must be bordered to know what is technology is behind the software they are using so that they can be sure of its security and related issues.

The bar chart shown below represents respondents' knowledge about protocols used in developing remote access software.

Table 9: Respondents' knowledge about protocols or technologies



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	38	56.7	56.7	56.7
	No	29	43.3	43.3	100.0
	Total	67	100.0	100.0	

Source: Field Survey, 2014

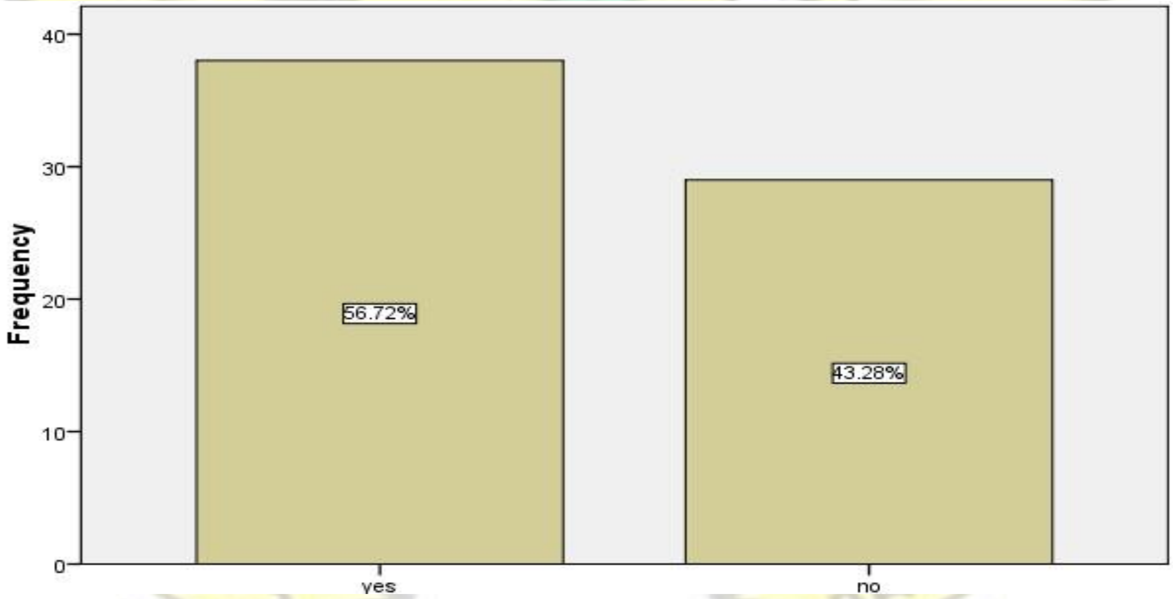


Figure 18: Respondents' knowledge about protocols or technologies. Source: Field Survey 2014

4.2.8 PROTOCOLS RESPONDENT KNOWS

As shown in table 10, 38 of the respondents representing 56.7 % of the total population had knowledge about the protocols used in developing remote access software while 29 of the respondents representing 43.3 % of the total population did not have knowledge about the protocols used in developing remote access software so were **not supposed to answer**.

Also, as shown in the table below 4.8, 3 of the respondents representing 4.5 % of the total respondents had knowledge about the Remote Frame Buffer (RFB), 9 of the respondents representing 13.4 of the respondents had knowledge about Remote Desktop Protocol (RDP), 3 of the respondents representing 4.5 % of the total population had knowledge about Pointto-Point Protocol (PPP). Also, 13 of the respondents representing 19.4 % of the total population had knowledge about RFB & RDP, 3 of the respondents representing 4.5 % of the total population also had about RFB & PPP, 4 of the respondents representing 6.0 % of the total population had knowledge about RDP & PPP. Furthermore, 3 of the respondents representing 4.5 % of the total population had knowledge about RFB, RDP & PPP.

However, when it comes to valid percentages, as shown in table 4.7 below, 3 of the respondents representing 7.9 % of the total valid responses had knowledge about the Remote Frame Buffer (RFB), 9 of the respondents representing 23.7 % of the total valid responses had knowledge about Remote Desktop Protocol (RDP), 3 of the respondents representing 7.9 % of the total valid responses had knowledge about Point-to-Point Protocol (PPP). Also, 13 of the respondents representing 34.2 % of the total valid responses had knowledge about RFB & RDP, 3 of the respondents representing 7.9 % of the total valid responses also had knowledge about RFB & PPP, and 4 of the respondents representing 10.5 % of the total valid responses had knowledge about RDP & PPP. Furthermore, 3 of the respondents representing 7.9 % of the total responses had knowledge about RFB, RDP & PPP.

The survey reveals that majority of the respondents are aware about the RFB and the RDP protocols.

Figure 19 below shows the protocols respondents are aware of.

Table 10: Protocols respondent knows

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	RFB	3	4.5	7.9	7.9
	RDP	9	13.4	23.7	31.6
	PPP	3	4.5	7.9	39.5
	RFB & RDP	13	19.4	34.2	73.7
	RFB & PPP	3	4.5	7.9	81.6
	RDP & PPP	4	6.0	10.5	92.1
	RFB, RDP & PPP	3	4.5	7.9	100.0
	Total	38	56.7	100.0	
Missing	not supposed to answer	29	43.3		
Total		67	100.0		

Source: Field Survey, 2014

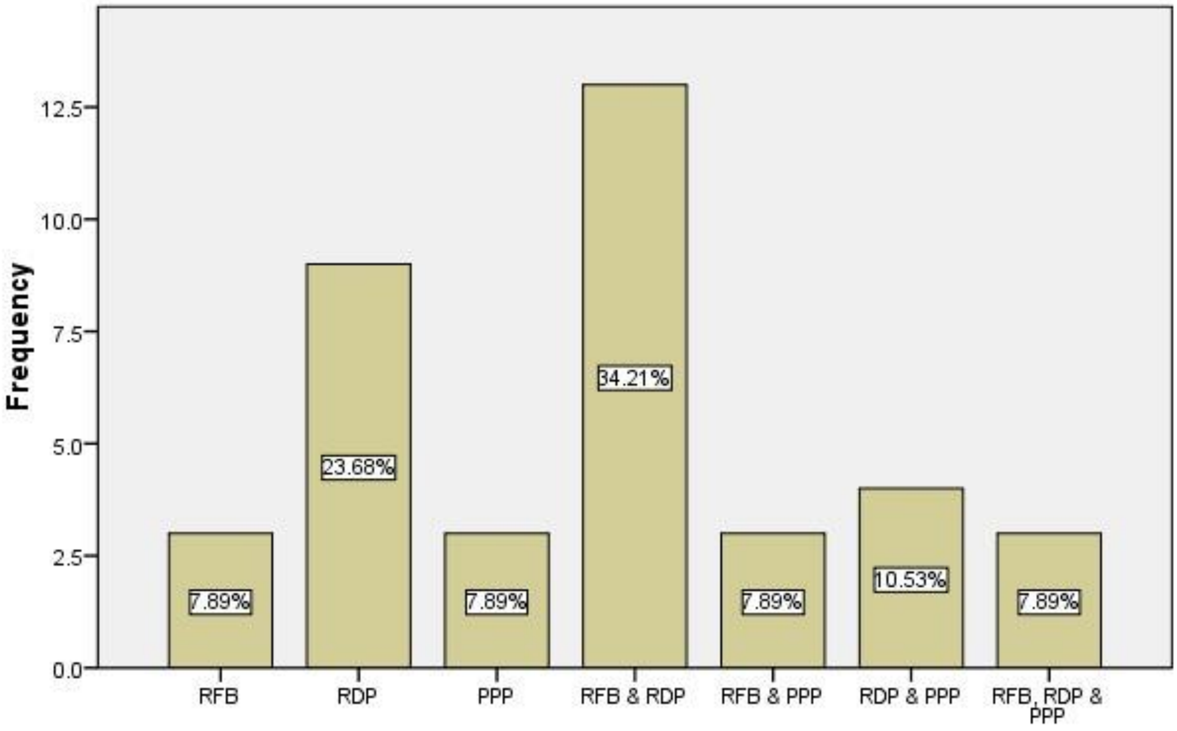


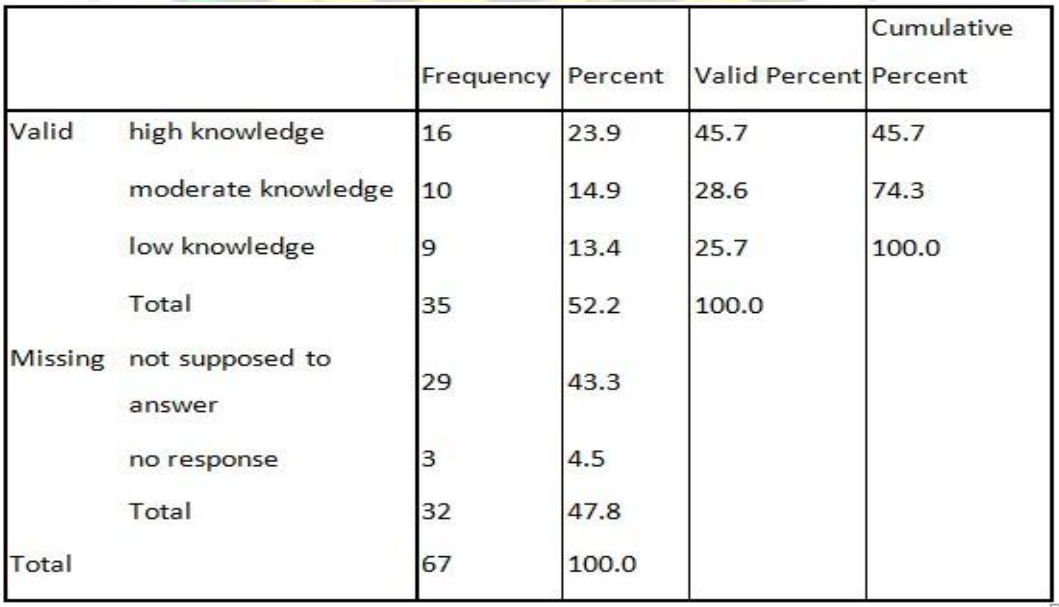
Figure 19: Protocols respondent knows. Source: Field Survey 2014

4.2.9 RATING RESPONDENTS' KNOWLEDGE ON PROTOCOLS

As shown in table 11, the valid responses out of the total population of 67 are 35 representing 52.2 % while the missing responses are 32 representing 47.8 % of the total population. However, as shown in table 4.8, out of the 32 missing responses, 29 respondents were actually **not supposed to answer** because they had earlier indicated they had no knowledge about the protocols and so their knowledge could not be rated and 3 respondents representing 4.5 % of the total population did not actually indicate any response though they had indicated earlier they had knowledge about the protocols. As shown in table 11, 16 of the respondents representing 23.9 % of the total respondents had high knowledge about the protocols, 10 of the respondents representing 14.9 % of total respondents had moderate knowledge about the protocols, and 9 of the respondents representing 13.4 % of the total respondents had low knowledge about the protocols. When it comes to valid percentages as shown in table 4.8, 16 of the respondents representing 45.7 % of the total valid responses had high knowledge about the protocols, 10 of the respondents representing 28.6 % of total valid responses had moderate knowledge about the protocols, and 9 of the respondents representing 25.7 % of the total valid responses had low knowledge about the protocols.

Figure 20 below shows a bar chart representing rating of respondents' knowledge on protocols.

Table 11: Rating respondents' knowledge on protocols



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high knowledge	16	23.9	45.7	45.7
	moderate knowledge	10	14.9	28.6	74.3
	low knowledge	9	13.4	25.7	100.0
	Total	35	52.2	100.0	
Missing	not supposed to answer	29	43.3		
	no response	3	4.5		
	Total	32	47.8		
Total		67	100.0		

Source: Field Survey, 2014

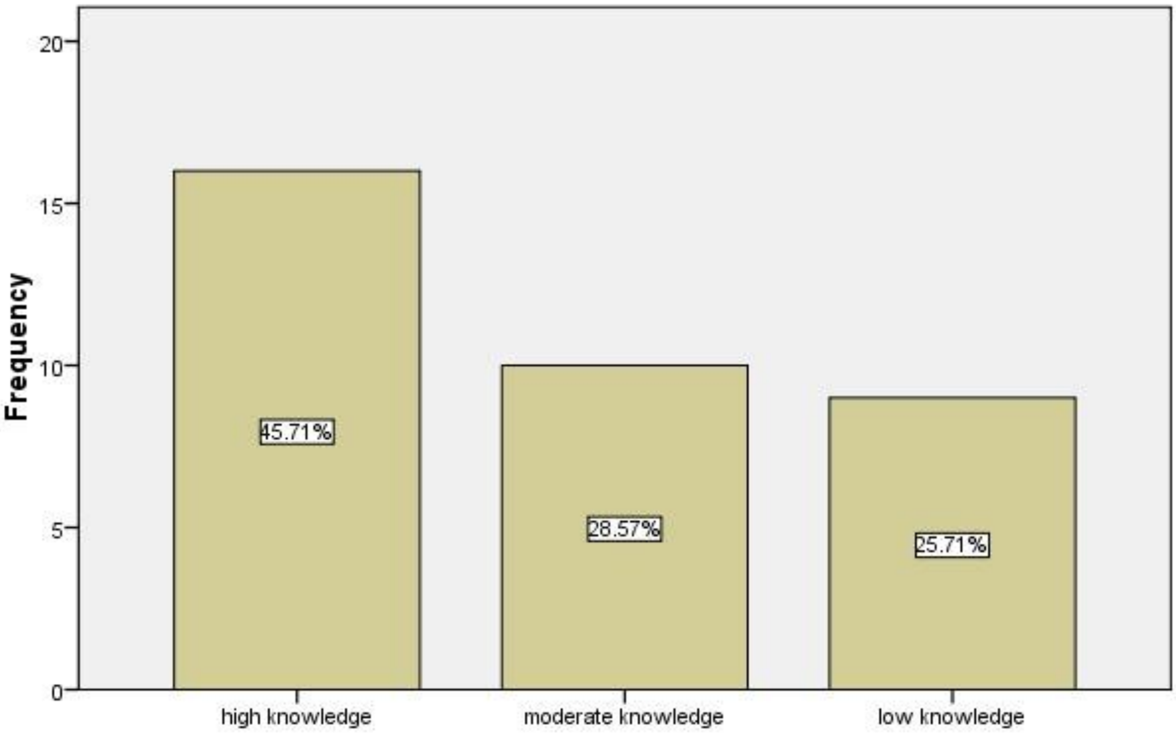


Figure 20: Rating respondents' knowledge on protocols. Source: Field Survey, 2014

4.2.10 REMOTE ACCESS SOFTWARE RESPONDENT HAS USED BEFORE

As shown in table 12, 51 of the respondents representing 76.1 % of the total population gave valid responses while 16 of the respondents representing 23.9 % of the total population did not give any response because they were **not supposed to answer** because they have never used any remote access software before.

As also shown in table 12, 2 of the respondents representing 3.9 % of the total population have ever used VNC, 25 of the respondents representing 37.3 % of the total population have ever used RD, 3 of the respondents representing 4.5 % of the total population have ever used TV, 8 of the respondents representing 11.9 % of the total respondents have ever used WRA, 6 of the respondents representing 9.0 % of the total population have ever used VNC & RD, 2 0f the representing 3.0 % of the total population and 3 of the respondents representing 4.5% of the total population have ever used VNC, RD & WRA.

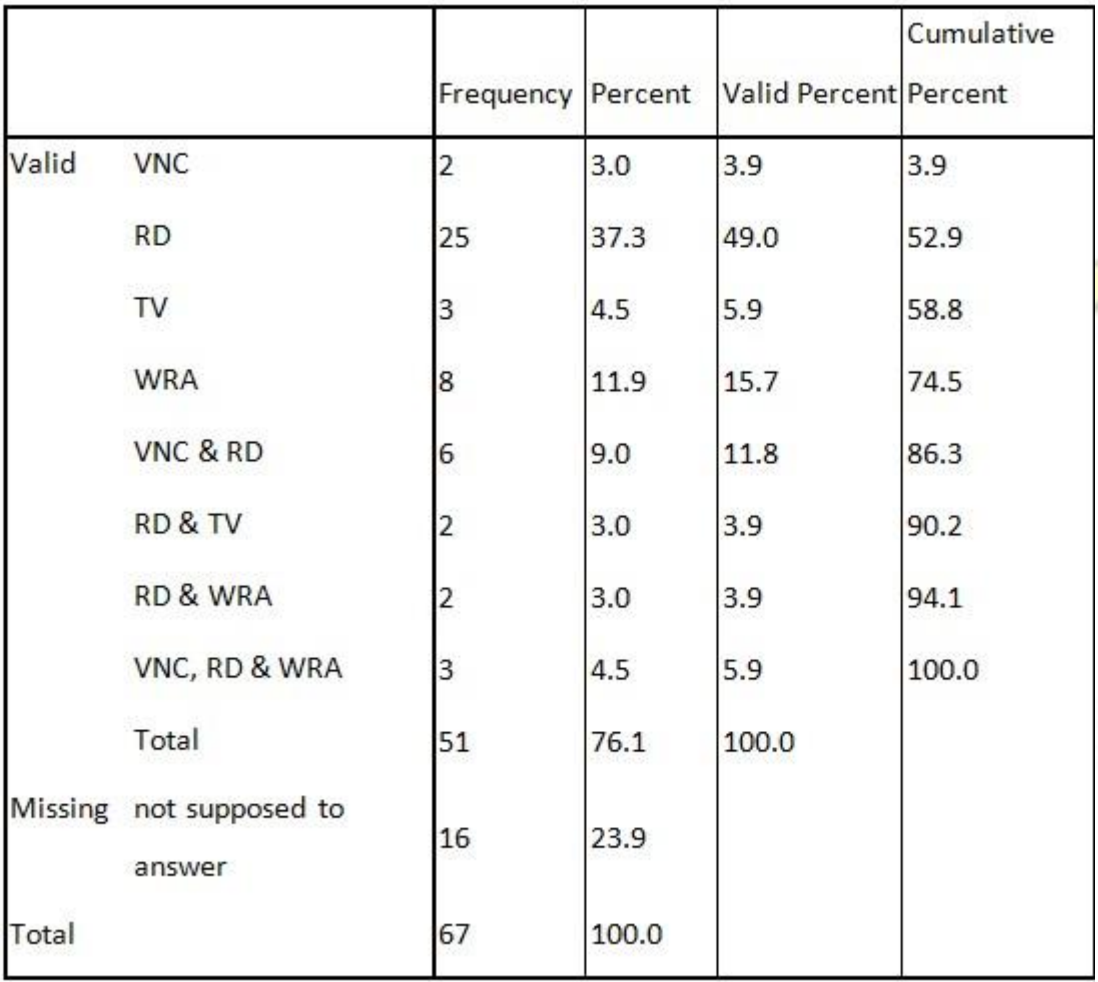
When it comes to valid percentages, 2 of the respondents representing 3.9 % of the total valid responses have ever used VNC, 25 of the respondents representing 49.0 % of the total valid responses have ever used RD, 3 of the respondents representing 5.9 % of the total valid responses have ever used TV, 8 of the respondents representing 15.7 % of the total valid responses have ever used WRA, 6 of the respondents representing 11.8 % of the total valid responses have ever used VNC & RD, 2 of the respondents representing 3.9 % of the total valid responses have ever used RD & TV, 2 of the respondents representing 3.9 % of the total valid responses have ever used RD & WRA and 3 of the respondents representing 5.9 % of the total valid responses have ever used VNC, RD and WRA.

From the study, it is very clear that Remote Desktop (RD) is the most popular remote access software with TeamViewer (TV) being the least popular remote access software.

The survey revealed that majority of the respondents use remote desktop.

Figure 21 represents remote access software respondent has used before.

Table 12: Remote access software respondent has used before



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	VNC	2	3.0	3.9	3.9
	RD	25	37.3	49.0	52.9
	TV	3	4.5	5.9	58.8
	WRA	8	11.9	15.7	74.5
	VNC & RD	6	9.0	11.8	86.3
	RD & TV	2	3.0	3.9	90.2
	RD & WRA	2	3.0	3.9	94.1
	VNC, RD & WRA	3	4.5	5.9	100.0
	Total	51	76.1	100.0	
Missing	not supposed to answer	16	23.9		
Total		67	100.0		

Source: Field Survey, 2014

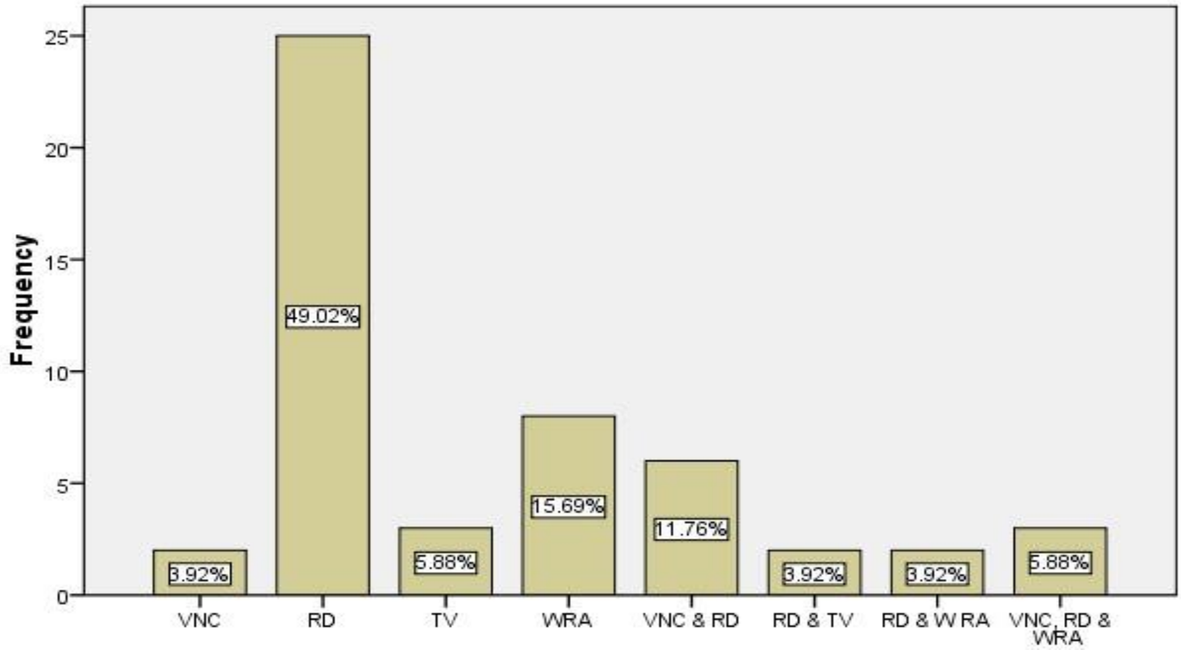


Figure 21: Remote Access software respondent has used before. Source: Field Survey, 2014

4.2.11 RESPONDENT'S INSPIRATION TO CONTINUALLY USE REMOTE SOFTWARE

As shown in table 13, 51 of the respondents representing 76.1 % of the total population gave valid responses while 16 of the respondents representing 23.9 % of the total population did not give any response because they were **not supposed to answer** because they have never used any remote access software before.

Also, as shown in table 4.11, 9 of the respondents representing 13.4 % of the total population have continually used their choice of remote access software because of it is **user friendly**, 17 of the respondents representing 25.4 % of the total population have continually used their choice of remote access software because of **adequate security in connection**, 17 of the respondents representing 25.4 % of the total population have continually used their choice of remote access software because of its **reliability** and 8 of the respondents representing 11.9 % of the total population have continually used their choice of remote access software because of its **performance**.

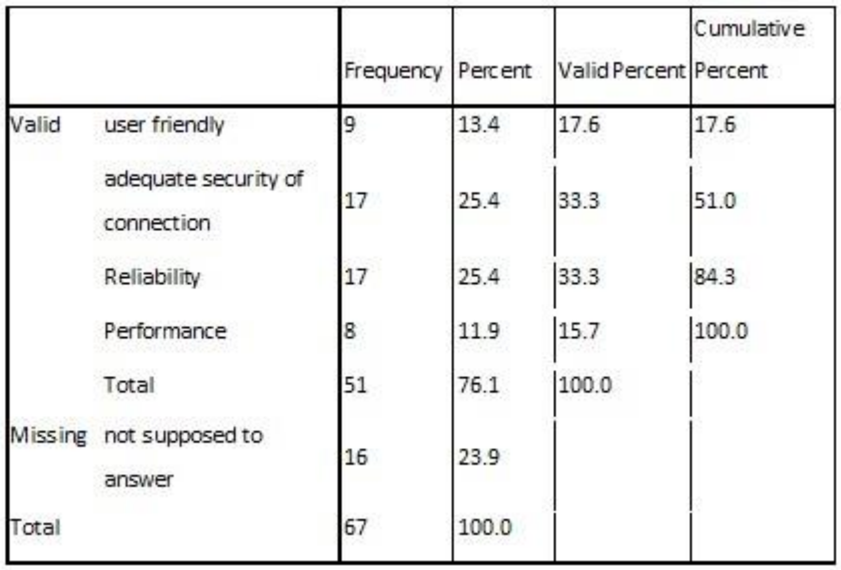
For valid percentages, 9 of the respondents representing 17.6 % of the valid responses have continually used their choice of remote access software because it is **user friendly**, 17 of the respondents representing 33.3 % of the valid responses have continually used their choice of remote access software because of **adequate security of connection**, 17 of the respondents representing 33.3 % of the valid responses have continually used their choice of remote access software because of its **reliability** and 8 of the respondents representing 15.7 % of the valid responses have continually used their choice of remote access software because of its **performance.**

From the study, the reason why users will continually use remote access software is split between **adequate security of connection** and **reliability**. So adequate security of connection and reliability are the most common reasons why users will continually use their choice of remote software.

The survey revealed that majority of the respondents are inspired by security of the remote access software to use them.

Figure 22 is a bar chart showing respondents' inspiration to continually use their choice of remote access software.

Table 13: Respondents inspiration to continually use remote software



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	user friendly	9	13.4	17.6	17.6
	adequate security of connection	17	25.4	33.3	51.0
	Reliability	17	25.4	33.3	84.3
	Performance	8	11.9	15.7	100.0
	Total	51	76.1	100.0	
Missing	not supposed to answer	16	23.9		
Total		67	100.0		

Source: Field Survey, 2014

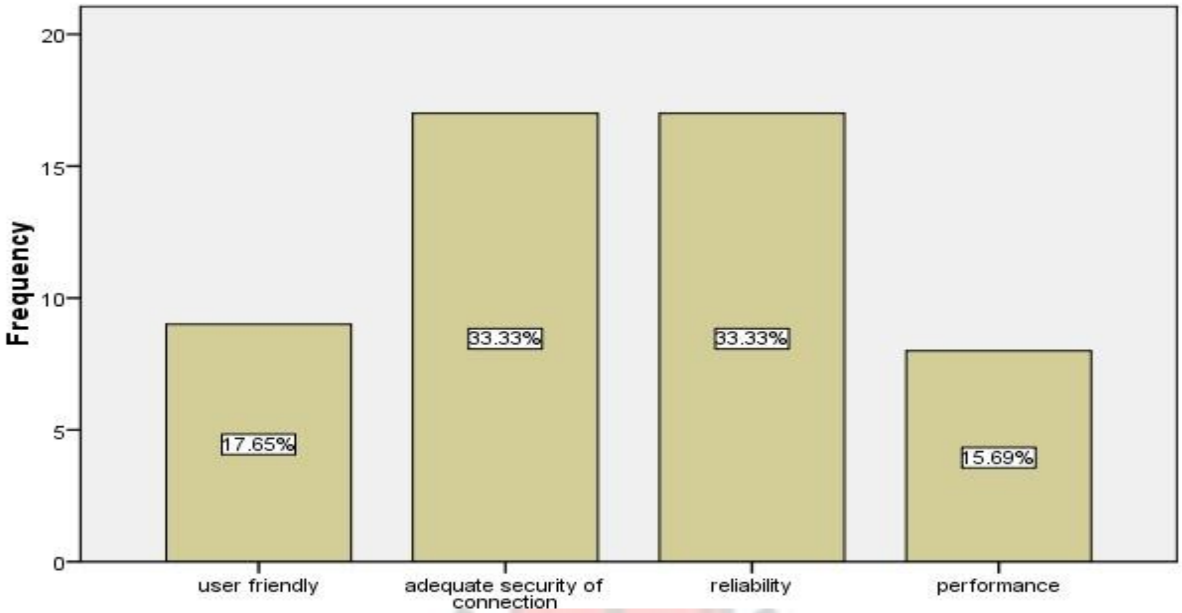


Figure 22: Respondents' inspiration to continually use remote software. Source: Field Survey, 2014

4.2.12 DOES RESPONDENT KNOW THE PROTOCOL THEIR CHOICE OF REMOTE SOFTWARE IS BASED ON?

As shown in table 14, 54 of the respondents representing 80.6 % of the total population gave valid responses while 13 of the respondents representing 19.4 % of the total population were **not supposed to answer** because they have never used any remote access software.

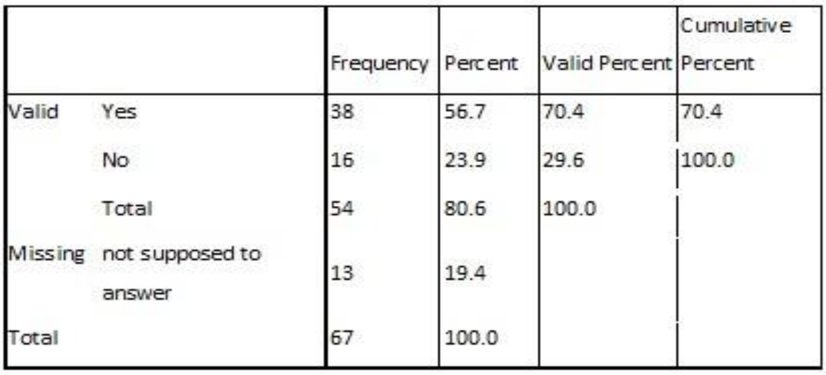
Also, as shown in table 4.12, 38 of the respondents representing 56.7 % of the total population had knew the protocols their choice of software are based on whiles 16 of the respondents representing 23.9 % of the total population did not know the protocols their choice of software were based on.

For valid percentages, 38 of the respondents representing 70.4 % of the total valid responses knew the protocols their choice of remote software were based on whiles 16 of the respondents representing 29.6 % of the total valid responses did not know the protocols their choice of software were based on.

The survey showed that majority of the respondents know the remote access protocol the their choice of remote access software is based.

Figure 23 below shows respondents' knowledge on protocols their choice of remote access software is based on.

Table 14: Does respondent know protocols their choice of software is based on



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	38	56.7	70.4	70.4
	No	16	23.9	29.6	100.0
	Total	54	80.6	100.0	
Missing	not supposed to answer	13	19.4		
Total		67	100.0		

Source: Field Survey, 2014

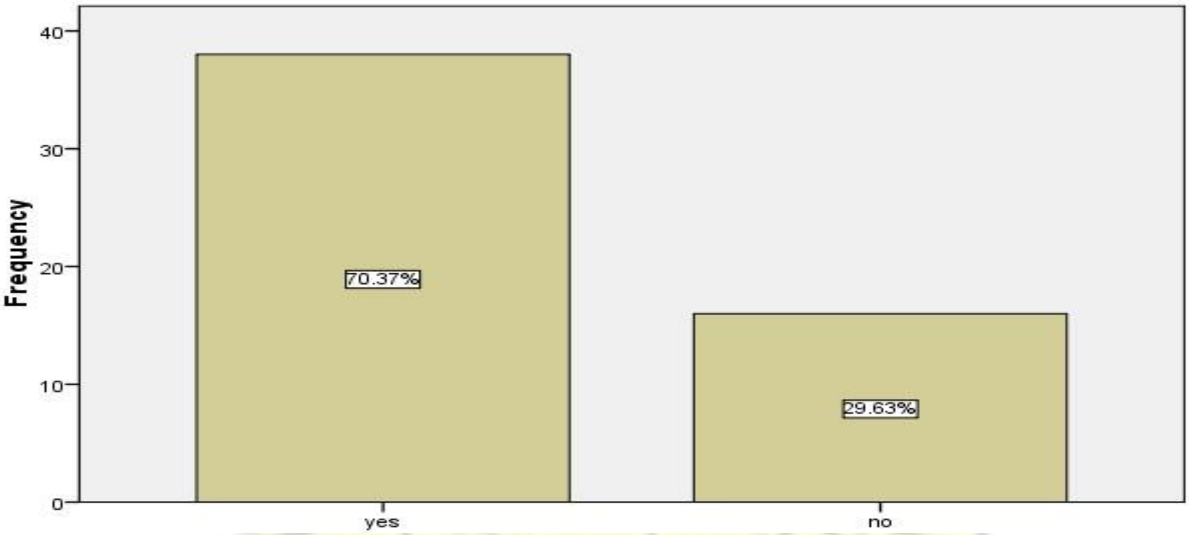


Figure 23: Does respondent know protocols their choice of software is based on? Source: Field Survey, 2014

4.2.13 PROTOCOL SOFTWARE IS BASED ON

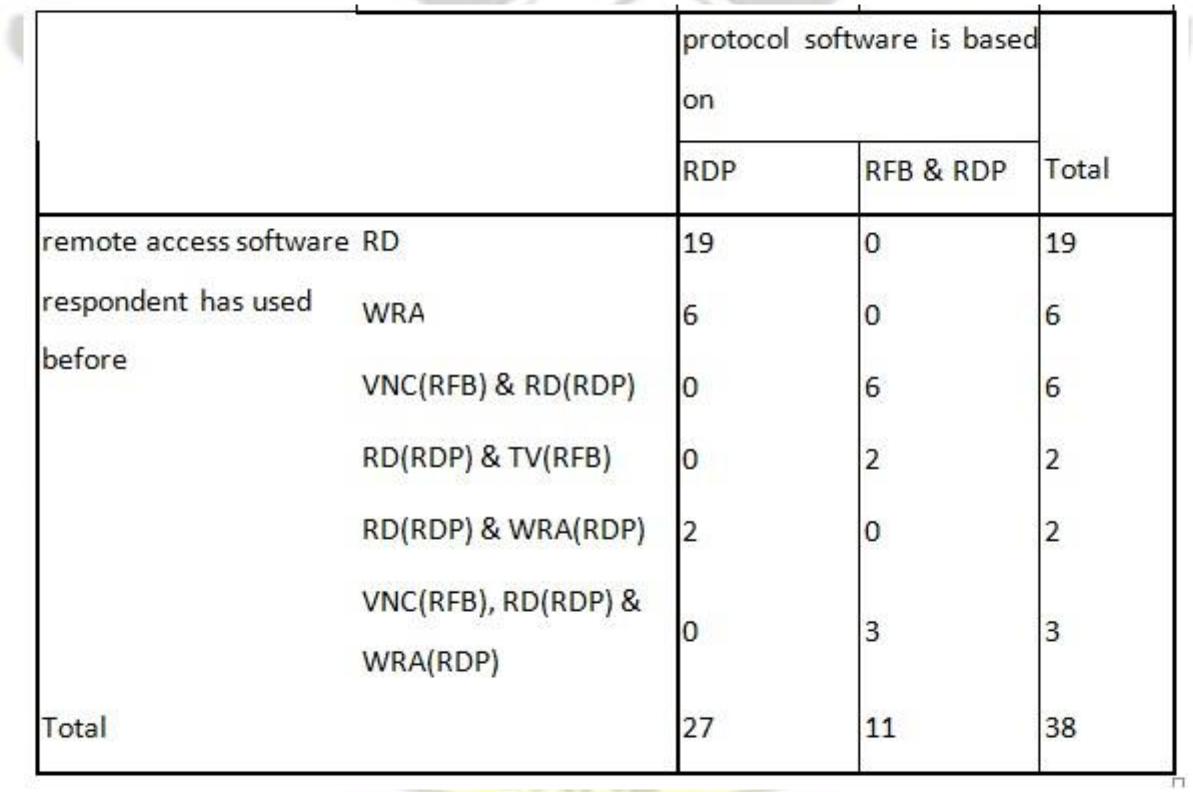
From table 15 shown below, 38 of the respondents representing 56.7 % of the total population actually knew the protocol their choice of remote access software is based on whiles 29 of the respondents representing 43.3 % of the total population were not supposed to answer because they did not have knowledge about these protocols.

From table 15 shown below, 19 respondents representing 50.0 % of the total valid responses indicated that RD (Remote Desktop) was based on the RDP (Remote Desktop Protocol), 6 of the respondents representing 15.8 % of the total valid responses indicated that WRA (Windows Remote Assistance) was based on the RDP, 6 of the respondents representing 15.8 % of the total valid responses who had used both VNC and RD indicated that VNC was based on RFB and RD was based on RDP, 2 of the respondents representing 5.3 % of the total valid responses who had used both RD and TV indicated that RD was based on RDP and TV was based on RFB, 2 of the respondents representing 5.3 % of the total valid responses indicated that both RD and WRA were both based on RDP. One of these 2 respondents actually indicated on the questionnaire that latest versions of Microsoft Windows like Windows 8 and 10 actually implemented RD and WRA using both RFB and RD. 3 of the respondents representing 7.9 % of the total valid responses who had used VNC, RD & WRA indicated that VNC was based on RFB and both RD & WRA were based RDP. From the research findings, it can be concluded RD is based on RDP, WRA is also based on RDP and VNC is based on RFB.

However, only 2 respondents indicated that TV is based on RFB which is inconclusive. From the survey, 38 of the 67 respondents knew the protocol their choice of remote access is based on.

The bar chart shown in figure 24 below represents the protocols the respondents choice of remote access software is software based.

Table 15: Protocol software is based



		protocol software is based on		Total
		RDP	RFB & RDP	
remote access software respondent has used before	RD	19	0	19
	WRA	6	0	6
	VNC(RFB) & RD(RDP)	0	6	6
	RD(RDP) & TV(RFB)	0	2	2
	RD(RDP) & WRA(RDP)	2	0	2
	VNC(RFB), RD(RDP) & WRA(RDP)	0	3	3
Total		27	11	38

Source: Field Survey, 2014

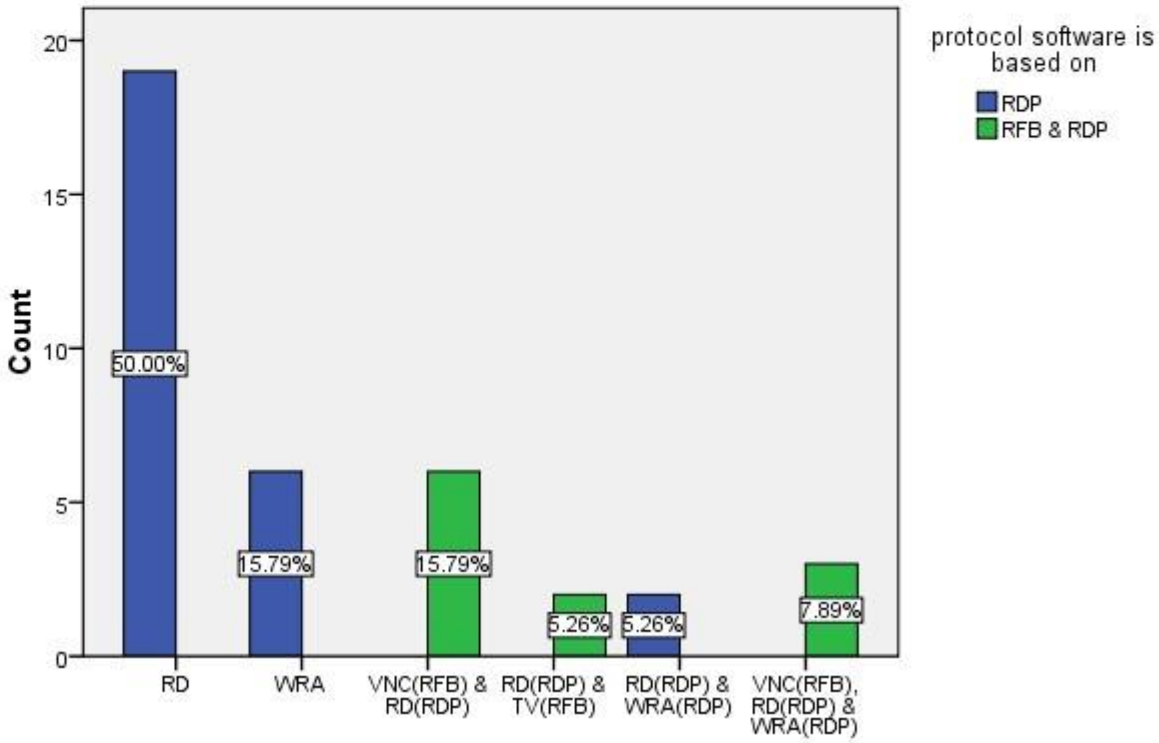


Figure 24: Protocol software is based on. Source: Field Survey, 2014

4.2.14 EFFICIENCY OF VNC

As shown in table 16, 6 of the respondents representing 9.0 % of the total population who had used VNC before indicated that the efficiency of VNC was **excellen**t, 2 of the respondent representing 3.0 % of the total population who had also used VNC but did not know the protocol it was based on also indicated that the efficiency of VNC was **good** and 3 of the respondents representing 4.5 % of the total population also indicated that the efficiency of VNC was **poor**.

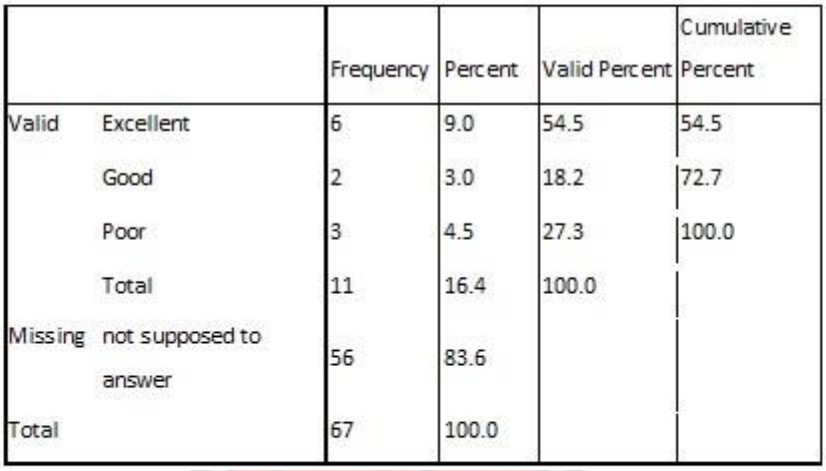
For valid responses, 6 of the respondents representing 54.5 % of the total valid responses indicated that the efficiency of VNC was **excellent**, 2 of the respondents representing 18.2 % of the total valid responses indicated that the efficiency of VNC was **good** and 3 of the respondents representing 27.3 % of the total valid responses indicated that the efficiency of VNC was **poor**.

56 of the respondents representing 83.6 % of the total population were not supposed to answer because they had never used VNC and so could not rate its efficiency.

Figure 25 below shows a bar chart representing the efficiency of VNC

From the survey, it can be concluded that VNC is efficient since out of the 11 respondents who had actually used VNC, 8 representing 72.72% rated it to be efficient.

Table 16: Efficiency of VNC



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	6	9.0	54.5	54.5
	Good	2	3.0	18.2	72.7
	Poor	3	4.5	27.3	100.0
	Total	11	16.4	100.0	
Missing	not supposed to answer	56	83.6		
Total		67	100.0		

Source: Field Survey, 2014

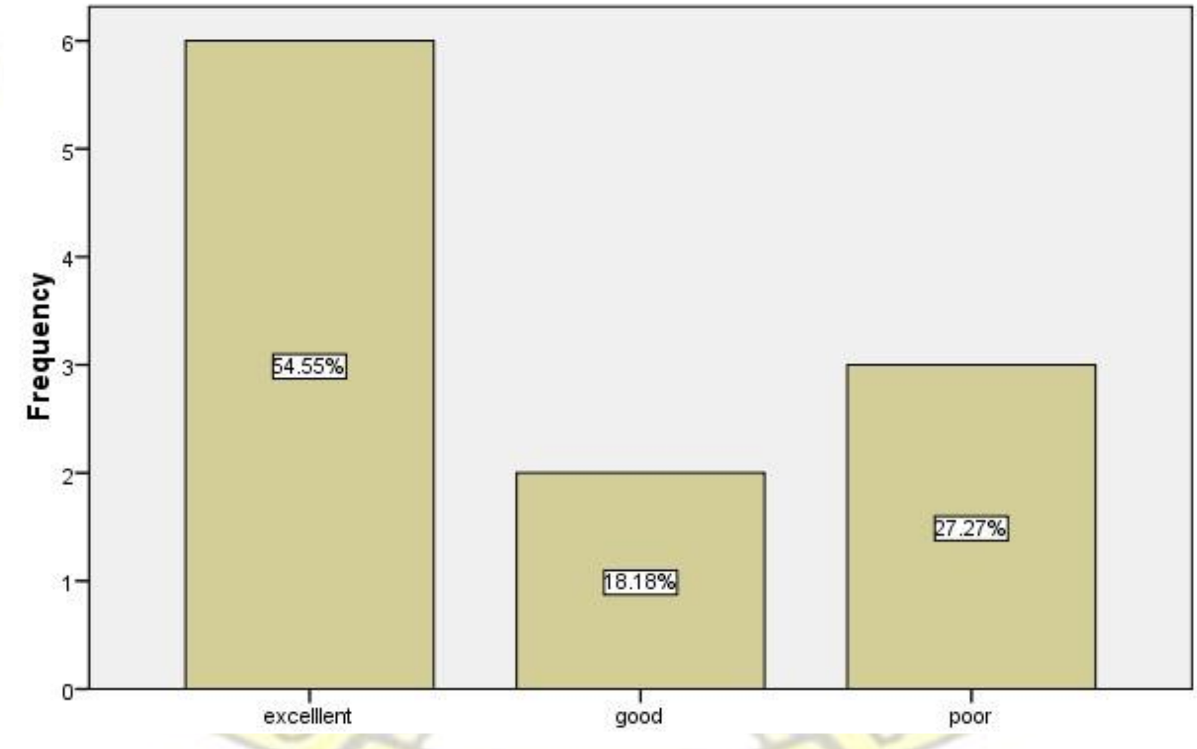


Figure 25: Efficiency of VNC. Source: Field Survey, 2014

4.2.15 RELIABILITY OF VNC

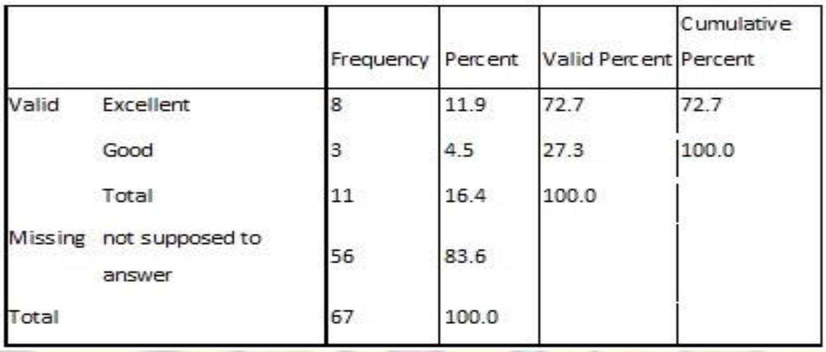
As indicated in table 17, 11 of the respondents representing 16.4 % of the total population had used VNC before and so could rate its reliability whiles 56 of the respondents representing 83.6 % of the total population were not supposed to answer because they had never used VNC and so could not rate its reliability.

From table 4.15 below, 8 of the respondents representing 11.9 % of the total population rated VNC's reliability as excellent and 3 of the respondents representing 4.5% of the total respondents rated VNC's reliability as being good.

Considering only the valid responses, 8 of the respondents representing 72.7 % of the valid total responses rated the reliability of VNC's reliability as excellent and 3 of the respondents representing 27.3 % of the total valid responses rated VNC's reliability as good.

The overall effect of these responses is that VNC is reliable. Figure 26 below is a bar chart showing how respondents rated the reliability of VNC.

Table 17: Reliability of VNC



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	8	11.9	72.7	72.7
	Good	3	4.5	27.3	100.0
	Total	11	16.4	100.0	
Missing	not supposed to answer	56	83.6		
Total		67	100.0		

Source: Field Survey, 2014

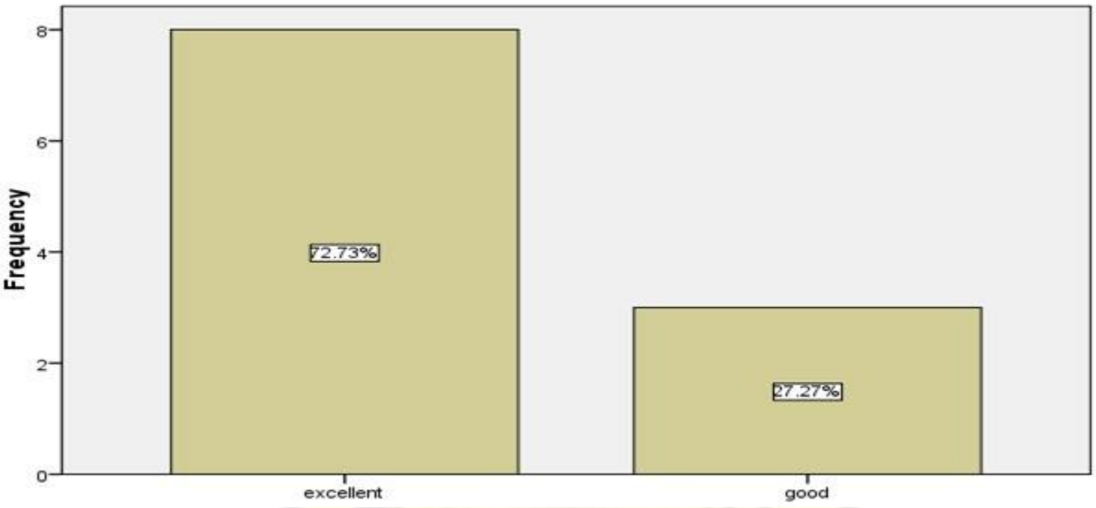


Figure 26: Reliability of VNC. Source: Field Survey, 2014

4.2.16 PERFORMANCE OF VNC

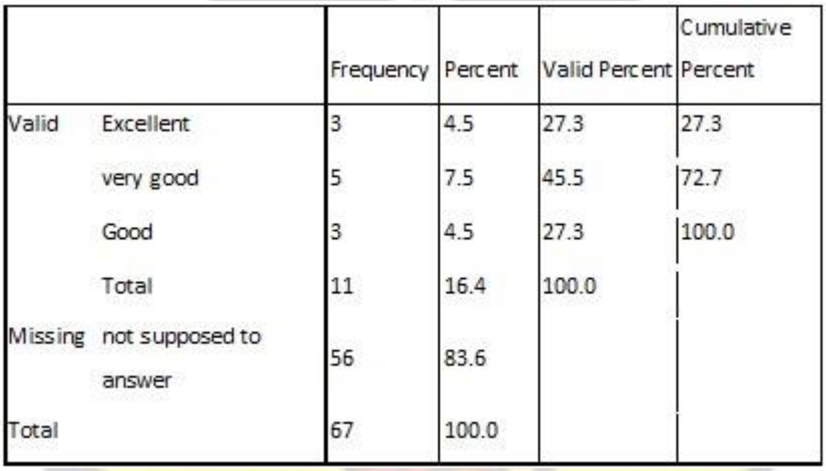
As indicated earlier, 11 of the respondents representing 16.4 % of the total population could rate the performance of VNC because they had used it before while 56 of the respondents, representing 83.6 % of the total population could not rate its performance because they had never used it before so were supposed to answer.

As indicated in table 18 below, 3 of the respondents representing 4.5% of the total population indicated the performance of VNC to be excellent, 5 of the respondents representing 7.5 % of the total population indicated that the performance of VNC was very good and 3 of the respondents representing 4.5 % of the total population indicated that the performance of VNC was good.

Considering only the valid responses, 3 of the respondents representing 27.3 % of the total valid responses indicated that the performance of VNC was excellent, 5 of the respondents representing 45.5 % of the total valid responses indicated that the performance of VNC is good.

The overall effect of these responses is that VNC performance is okay.

Table 18: Performance of VNC



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	3	4.5	27.3	27.3
	very good	5	7.5	45.5	72.7
	Good	3	4.5	27.3	100.0
	Total	11	16.4	100.0	
Missing	not supposed to answer	56	83.6		
Total		67	100.0		

Source: Field Survey, 2014

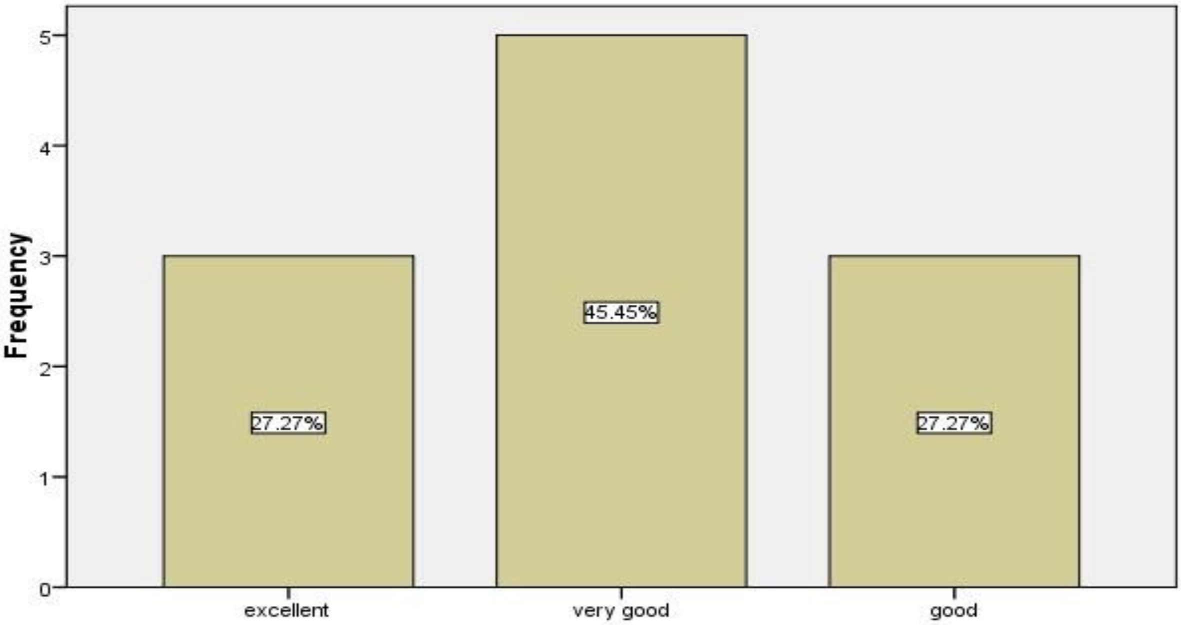


Figure 27: Performance of VNC. Source: Field Survey, 2014

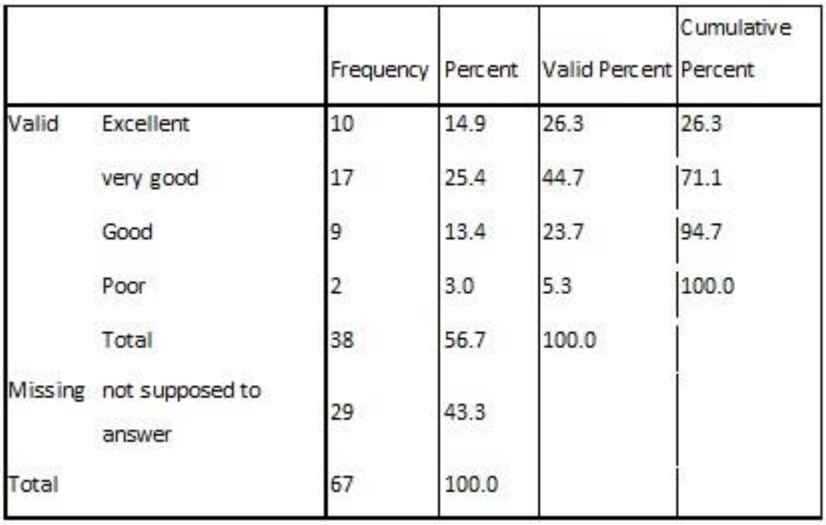
4.2.17 EFFICIENCY OF RD

As shown in table 19, 38 of the respondents representing 56.7 % of the total population had actually used RD and so could rate its efficiency while 29 of the respondents representing 43.3 % of the total population had never used RD and so could not rate its efficiency.

Also, as shown in table 19, 10 of the respondents representing 14.9 % of the total population indicated that RD was efficient, 17 of the respondents representing 25.4 % of the total population indicated that the efficiency of RD was very good and 2 of the respondents representing 3.0 % of the total population indicated that the efficiency of RD was poor. Considering only the valid responses, 10 of the respondents representing 26.3 % of the total valid responses answered that the efficient of RD was excellent, 17 of the respondents representing 44.7 % of the total valid responses answered that the efficiency of RD was very good and 2 of the respondents representing 5.3 of the total valid responses answered that the efficiency of RD was poor.

Figure 28 shows a bar chart representing the efficiency of Remote Desktop (RD) From the study, majority of the respondents are of the view that RD is efficient.

Table 19: Efficiency of Remote Desktop



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	10	14.9	26.3	26.3
	very good	17	25.4	44.7	71.1
	Good	9	13.4	23.7	94.7
	Poor	2	3.0	5.3	100.0
	Total	38	56.7	100.0	
Missing	not supposed to answer	29	43.3		
Total		67	100.0		

Source: Field Survey, 2014

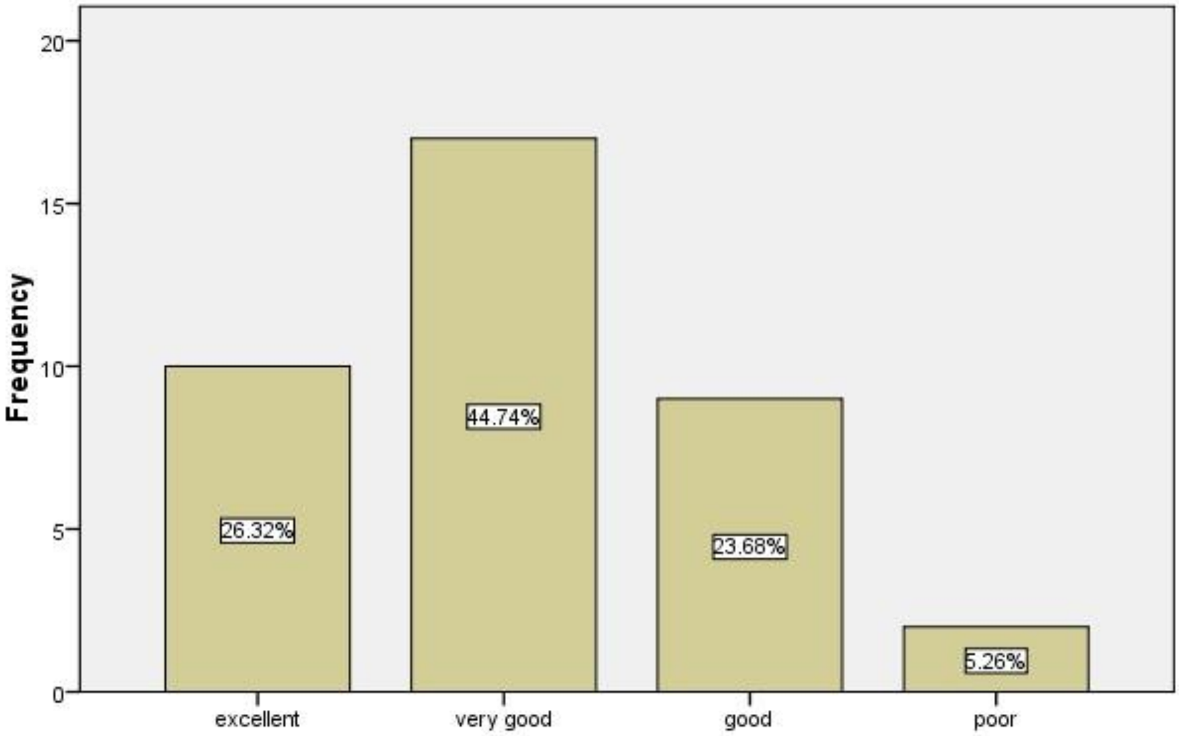


Figure 28: Efficiency of remote desktop. Source: Field Survey, 2014

4.2.18 RELIABILITY OF REMOTE DESKTOP (RD)

As shown in table 20, 38 of the respondents representing 56.7 % of the total population gave valid responses and 29 of the respondents representing 43.3 % of the total population did not give any response because they were not supposed to answer since they had never used remote desktop before.

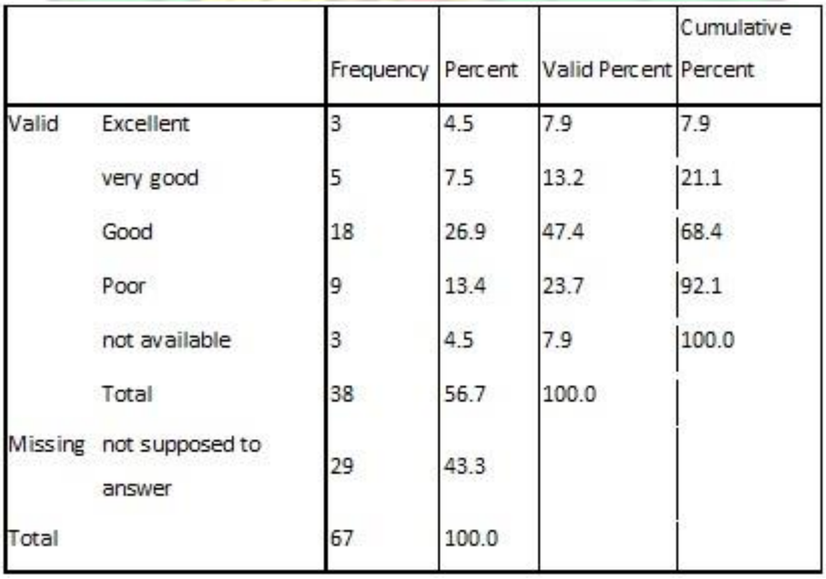
From table 4.18 below, 3 of the respondents representing 4.5 % of the total population rated the reliability of remote desktop as excellent, 5 of the respondents representing 7.5 % of the total population rated the reliability of remote desktop as very good, 18 of the respondents representing 26.9 % of the total population rated the reliability of remote desktop as good, 9 of the respondents representing 13.4 % of the total population rated the reliability of remote desktop as poor and 3 respondents representing 4.5 % of the total population rate the reliability of remote desktop as not available since they did not know about the reliability of remote desktop.

Considering only valid responses, 3 of the respondents representing 7.9 % of the total valid responses rated the reliability of remote desktop as excellent, 5 of the respondents representing 13.2 % of the total valid responses rated the reliability of remote desktop as very good, 18 of the respondents representing 47.4 % of the total valid responses rated the reliability of remote desktop as good, 9 of the respondents representing 23.7 % of the total valid responses rated the reliability of remote desktop as poor and 3 of the respondents representing 7.9 % of the total valid responses rated the reliability of remote desktop as not available since they did not know about its reliability.

From the study, majority of the respondents are of the view that RD is reliable.

Figure 29 is a bar chart showing the reliability of remote desktop.

Table 20: Reliability of Remote Desktop



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	3	4.5	7.9	7.9
	very good	5	7.5	13.2	21.1
	Good	18	26.9	47.4	68.4
	Poor	9	13.4	23.7	92.1
	not available	3	4.5	7.9	100.0
	Total	38	56.7	100.0	
Missing	not supposed to answer	29	43.3		
Total		67	100.0		

Source: Field Survey, 2014

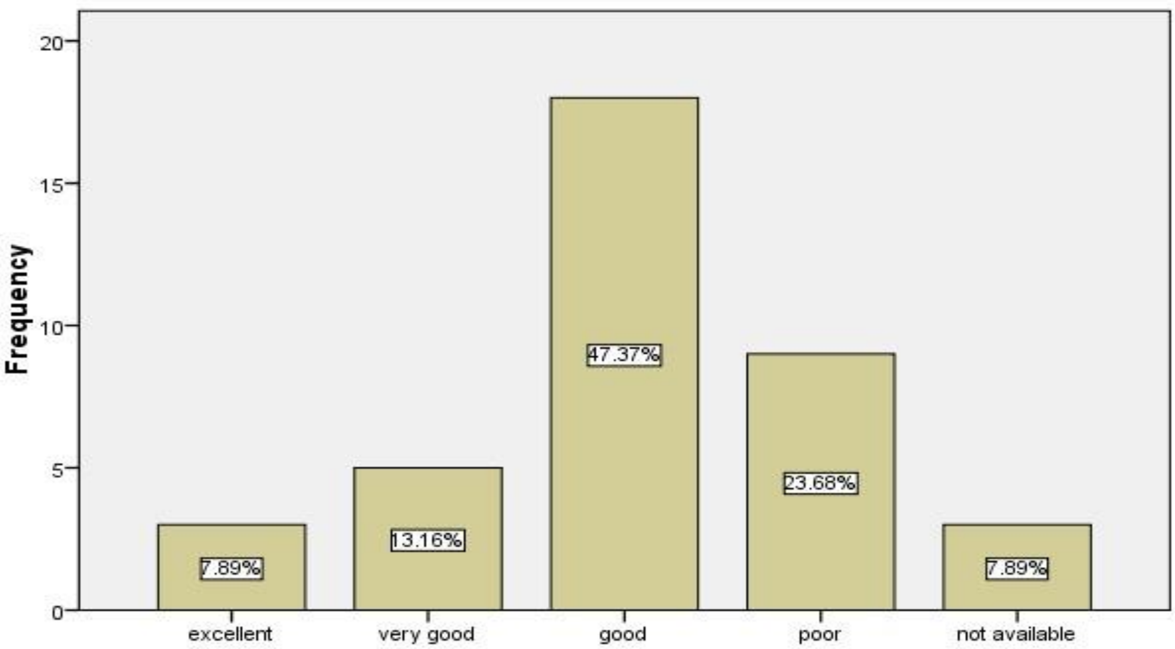


Figure 29: Reliability of remote desktop. Source: Field Survey, 2014

4.2.19 PERFORMANCE OF REMOTE DESKTOP

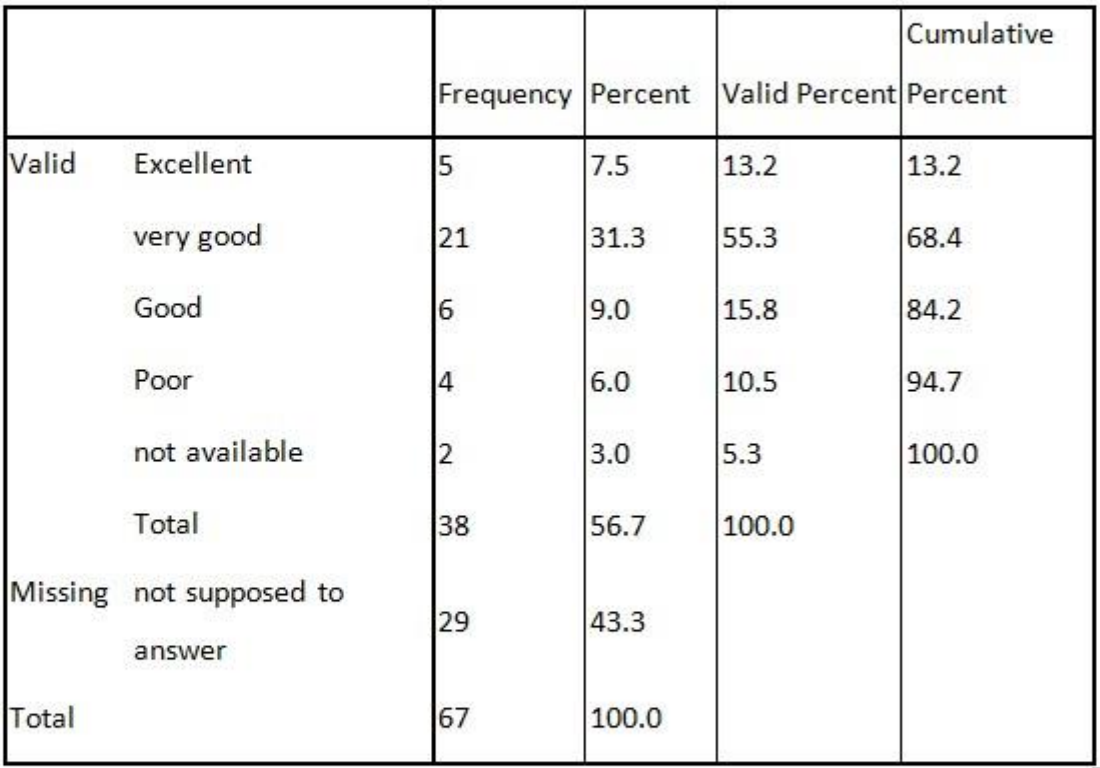
As shown in table 21 below, 38 of the respondents representing 56.7 % of the total population gave valid responses while 29 of the respondents representing 43.3 % of the total population did not indicate any response because they were not supposed to since they have never used remote desktop.

Table 4.19 further indicates that 5 of the respondents representing 7.5 % of the total population rated the performance of remote desktop as being excellent, 21 of the respondents representing 31.3 % of the total population rated the performance of remote desktop as being very good, 6 of the respondents representing 9.0 % of the total population rated the performance of remote desktop as being good, 4 respondents representing 6.0 % of the total population rated the performance of remote desktop as being poor and 2 of the respondents representing 3.0 % of the total population rated the performance of remote desktop as not available because they did not have knowledge about its performance. Looking at only the valid responses, 5 of the respondents representing 13.2 % of the total valid responses rated the performance of remote desktop as being excellent, 21 of the respondents representing 55.3 % of the total valid responses rated the performance of remote desktop as very good, 6 of the respondents representing 15.8 % of the total valid responses rated the performance of remote desktop as good, 4 of the respondents representing 10.5 % of the total valid responses rated the performance of remote desktop as poor and 2 of the respondents representing 5.3 % of the total valid responses rated the performance of remote desktop as not available because they did not have knowledge about its performance.

Figure 30 is a bar chart showing the performance of remote desktop.

From the study, majority of the respondents agreed that the performance of remote desktop is very good.

Table 21: Performance of remote desktop



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	5	7.5	13.2	13.2
	very good	21	31.3	55.3	68.4
	Good	6	9.0	15.8	84.2
	Poor	4	6.0	10.5	94.7
	not available	2	3.0	5.3	100.0
	Total	38	56.7	100.0	
Missing	not supposed to answer	29	43.3		
Total		67	100.0		

Source: Field Survey, 2014

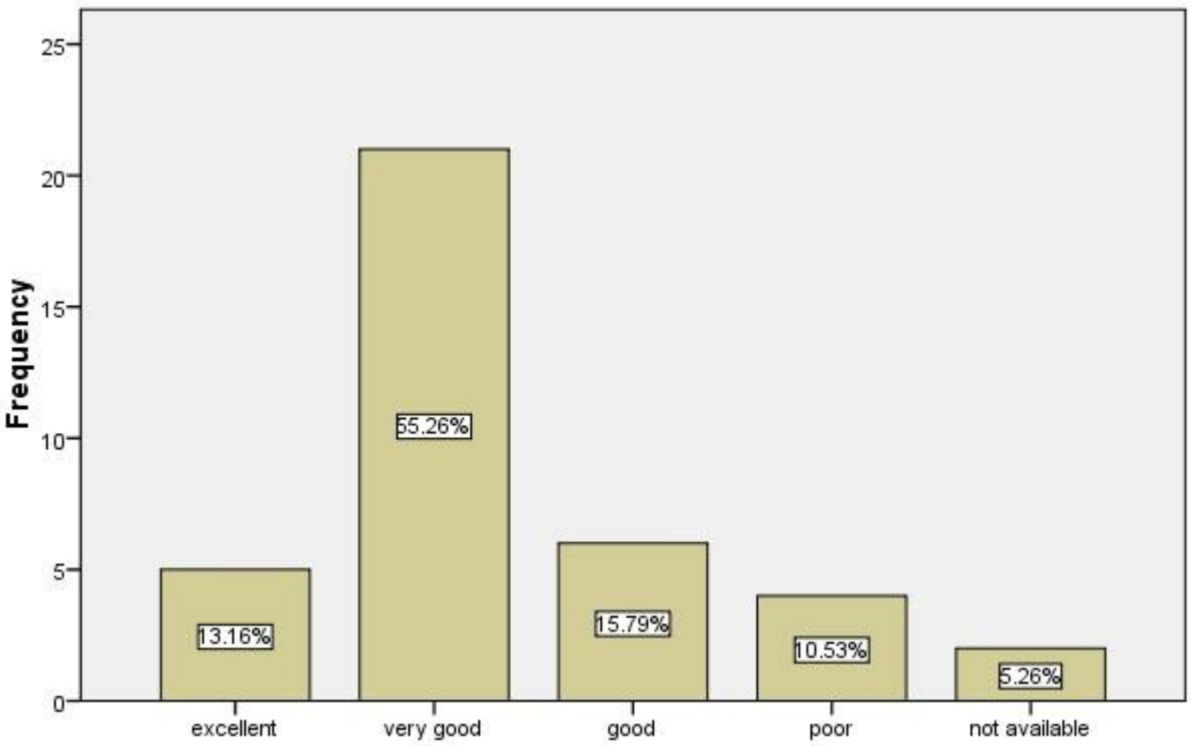


Figure 30: Performance of remote desktop. Source: Field Survey, 2014

4.2.20 EFFICIENCY OF TEAMVIEWER

As indicated in table 22, 5 of the respondents representing 7.5 % of the total population gave valid responses while 62 of the respondents representing 92.5 % of the total population did not indicate any response because they were not supposed to answer since they have never used TeamViewer before.

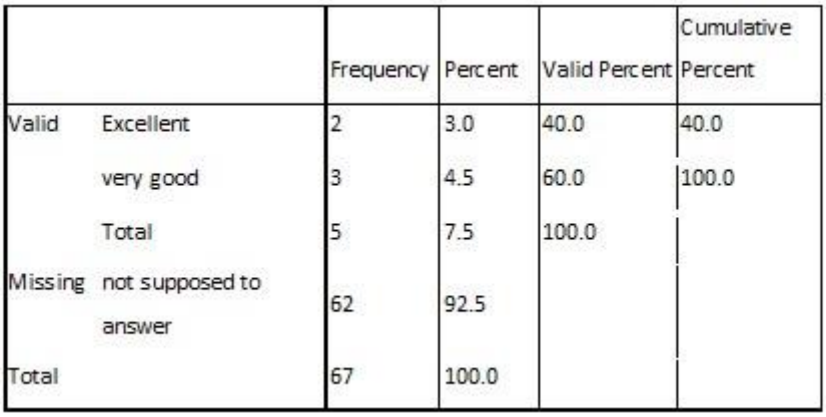
Table 22 shows that 2 of the respondents representing 3.0 % of the total population rated the efficiency of TeamViewer as being excellent and 3 of the respondents representing 4.5 % of the total population indicated that the efficiency of TeamViewer was very good.

Looking at valid responses alone, 2 of the respondents representing 40.0 % of the total valid responses indicated that the efficiency of TeamViewer was excellent and 3 of the respondents representing 60.0 % of the total valid responses indicated that the efficiency of TeamViewer was very good.

Majority of the respondents agreed that the efficiency of TeamViewer was very good.

Figure 31 is a bar chart illustrating the efficiency of TeamViewer.

Table 22: Efficiency of TeamViewer



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	2	3.0	40.0	40.0
	very good	3	4.5	60.0	100.0
	Total	5	7.5	100.0	
Missing	not supposed to answer	62	92.5		
Total		67	100.0		

Source: Field Survey, 2014

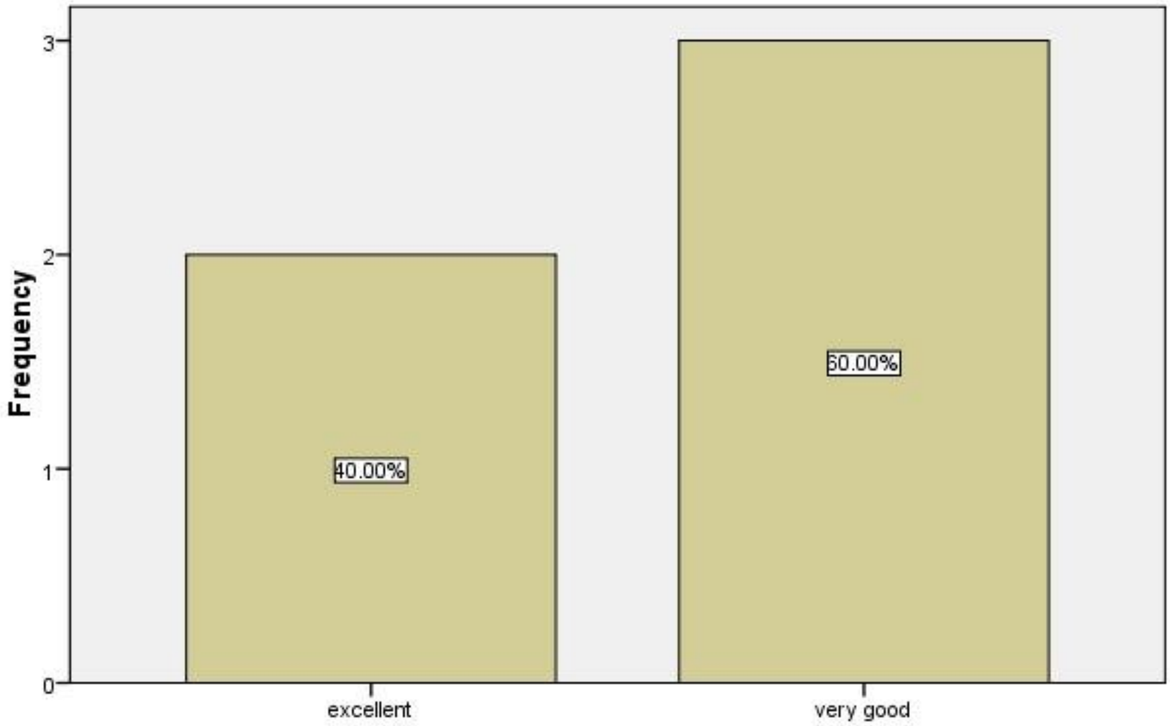


Figure 31: Efficiency of Teamviewer. Source: Field Survey, 2014

4.2.21 RELIABILITY OF TEAMVIEWER

As indicated in table 23, 5 of the respondents representing 7.5 % of the total population gave valid responses while 62 of the respondents representing 92.5 % of the total population did not indicate any response because they were not supposed to answer since they have never used TeamViewer before.

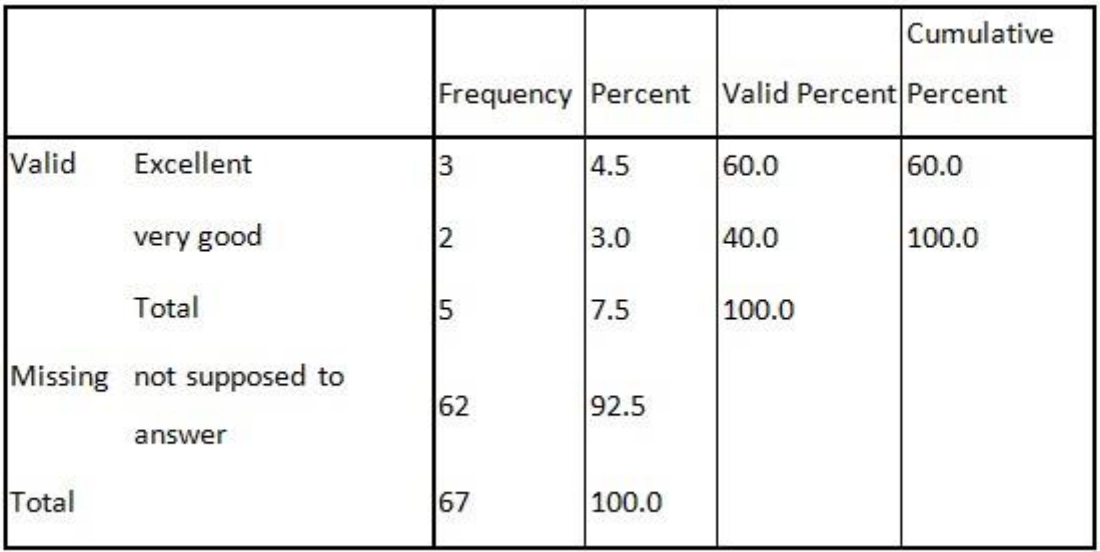
Table 23 shows that 3 of the respondents representing 4.5 % of the total population rated the reliability of TeamViewer as being excellent and 2 of the respondents representing 3.0 % of the total population indicated that the reliability of TeamViewer was very good.

Looking at valid responses alone, 3 of the respondents representing 60.0 % of the total valid responses indicated that the reliability of TeamViewer was excellent and 2 of the respondents representing 40.0 % of the total valid responses indicated that the reliability of TeamViewer was very good.

Majority of the respondents agreed that the reliability of teamviewer was excellent.

Figure 32 is a bar chart illustrating the reliability of TeamViewer.

Table 23: Reliability of TeamViewer



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	3	4.5	60.0	60.0
	very good	2	3.0	40.0	100.0
	Total	5	7.5	100.0	
Missing	not supposed to answer	62	92.5		
Total		67	100.0		

Source: Field Survey, 2014

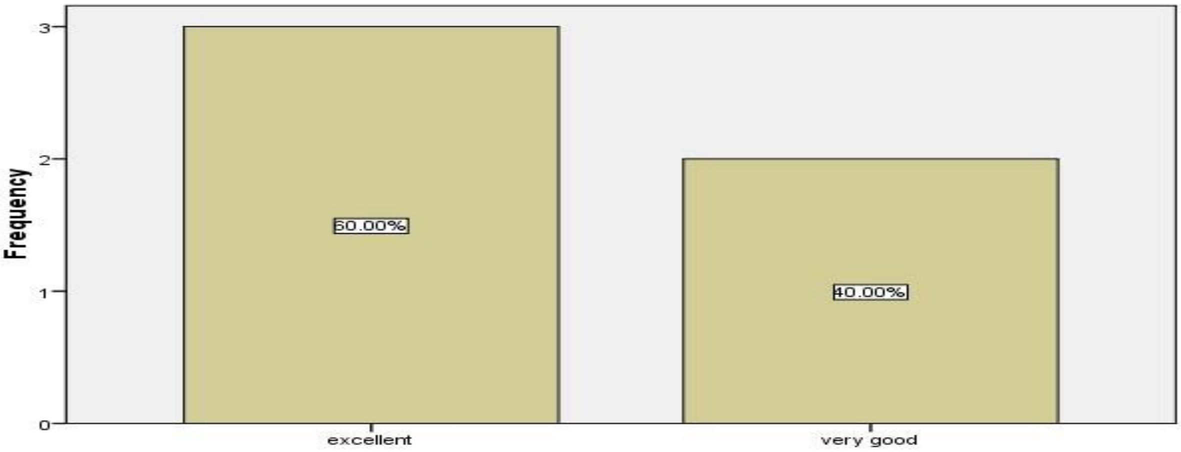


Figure 32: Reliability of TeamViewer. Source: Field Survey, 2014

4.2.22 PERFORMANCE OF TEAMVIEWER

As indicated in table 24, 5 of the respondents representing 7.5 % of the total population gave valid responses while 62 of the respondents representing 92.5 % of the total population did not indicate any response because they were not supposed to answer since they have never used TeamViewer before.

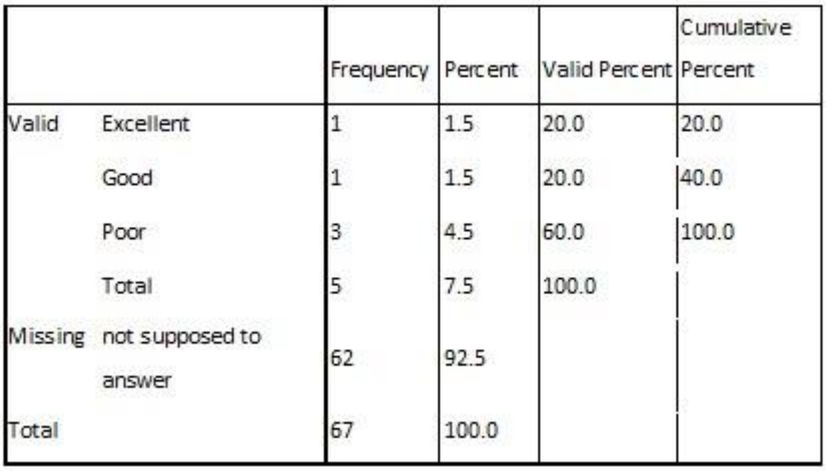
Also, in table 24, 1 of the respondents representing 1.5 % of the total population rated the performance of TeamViewer as being excellent, 1 of the respondents representing 1.5 % of the total population rated the performance of TeamViewer as being good and 3 of the respondents representing 4.5 % of the total population indicated the performance of TeamViewer as being poor.

Looking at only the valid responses, 1 of the respondents representing 20.0 % of the total valid responses rated the performance of TeamViewer as being excellent, 1 of the respondents representing 20.0 % of the total responses rated the performance of TeamViewer as being good and 3 of the respondents representing 60.0 % of the total population indicated the performance of TeamViewer as being poor.

Figure 33 is a bar chart showing the performance of TeamViewer.

As can be seen from the study, majority of the respondents agreed that the performance of TeamViewer was poor.

Table 24: Performance of TeamViewer



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	1	1.5	20.0	20.0
	Good	1	1.5	20.0	40.0
	Poor	3	4.5	60.0	100.0
	Total	5	7.5	100.0	
Missing	not supposed to answer	62	92.5		
Total		67	100.0		

Source: Field Survey, 2014

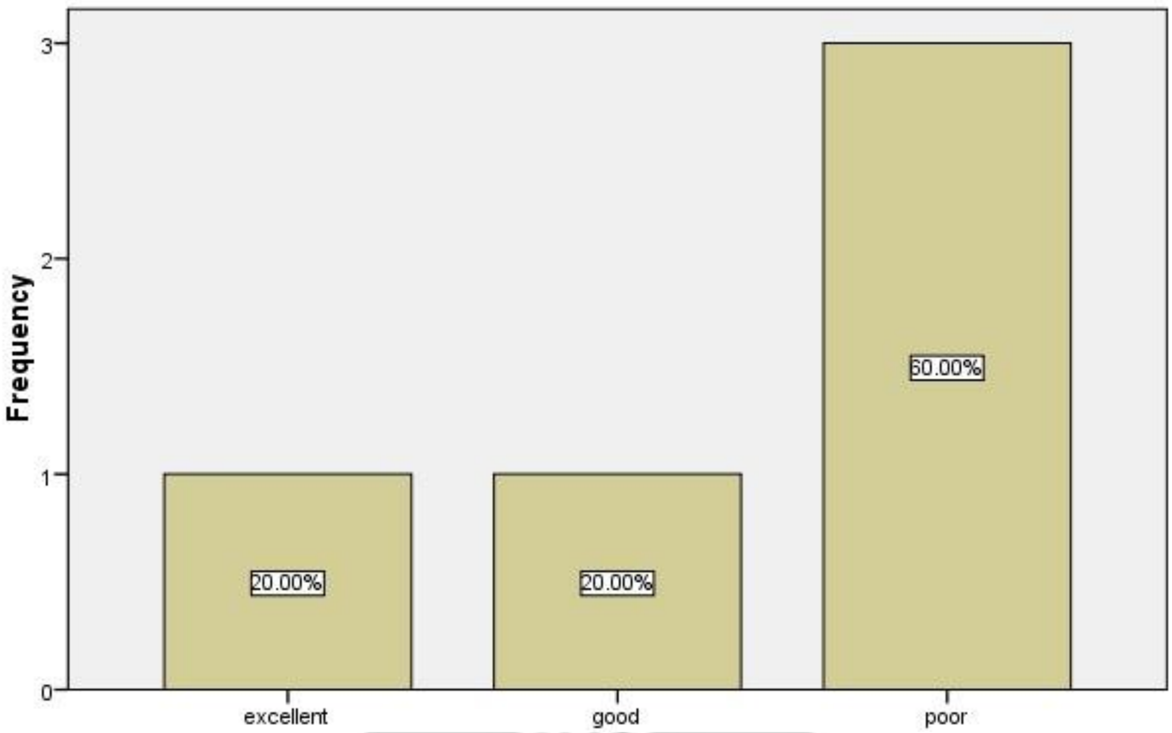


Figure 33: Performance of TeamViewer. Source: Field Survey, 2014

4.2.23 EFFICIENCY OF WINDOWS REMOTE ASSISTANCE (WRA)

As shown in table 25, 13 of the respondents representing 19.4 % of the total population gave valid responses while 54 of the respondents representing 80.6 % of the total population did not give any response because they were not supposed to answer since they have never used WRA before.

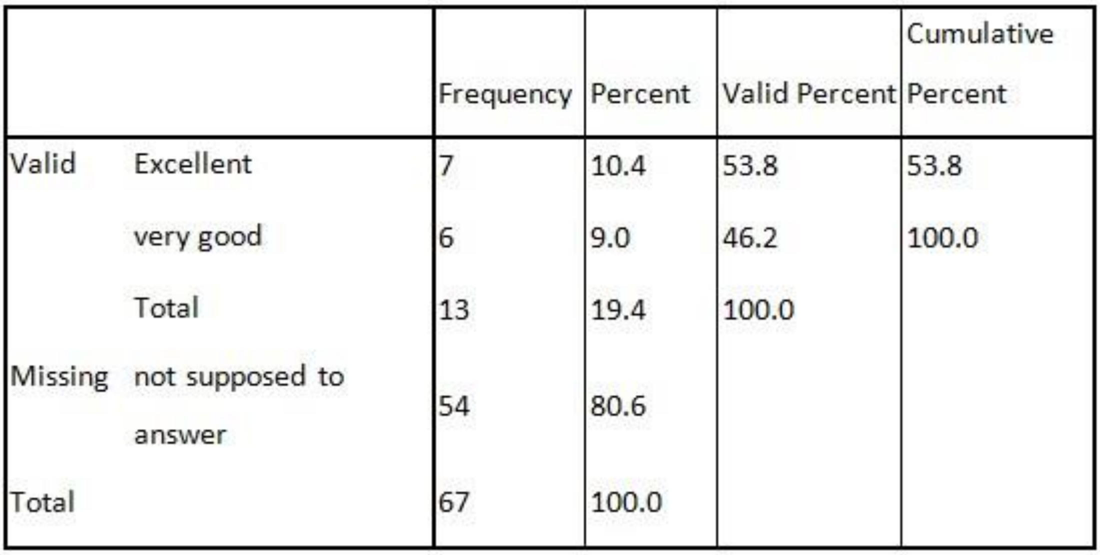
From table 25 below, 7 of the respondents representing 10.4 % of the total population rated the efficiency of WRA as excellent and 6 of the respondents representing 9.0 % of the total population rated the efficiency of WRA as very good.

Considering only the valid responses, 7 of the respondents representing 53.8 % of the total valid responses rated the efficiency of WRA as excellent and 6 of the respondents representing 46.2 % of the total valid responses rated the efficiency of WRA as very good.

Majority of the respondents agreed that the efficiency of WRA was excellent.

Figure 34 represents a bar chart illustrating the efficiency of WRA.

Table 25: Efficiency of Windows Remote Assistance (WRA)



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	7	10.4	53.8	53.8
	very good	6	9.0	46.2	100.0
	Total	13	19.4	100.0	
Missing	not supposed to answer	54	80.6		
Total		67	100.0		

Source: Field Survey, 2014

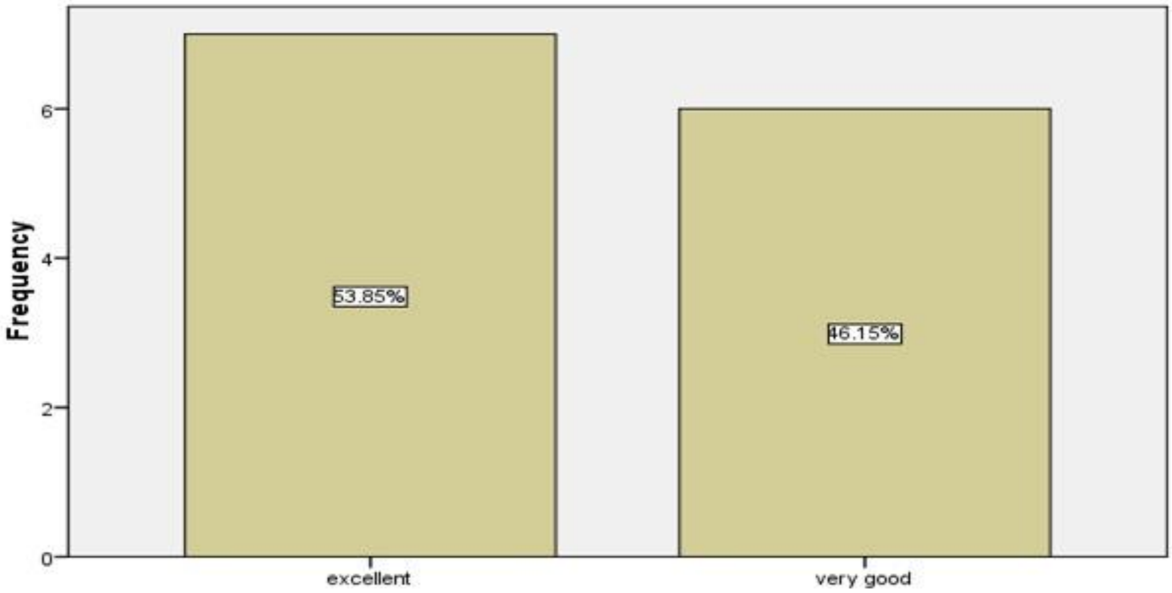


Figure 34: Efficiency of Windows Remote Assistance. Source: Field Survey, 2014

4.2.24 RELIABILITY OF WINDOWS REMOTE ASSISTANCE

As shown in table 26, 13 of the respondents representing 19.4 % of the total population gave valid responses while 54 of the respondents representing 80.6 % of the total population did not give any response because they were not supposed to answer since they have never used WRA before.

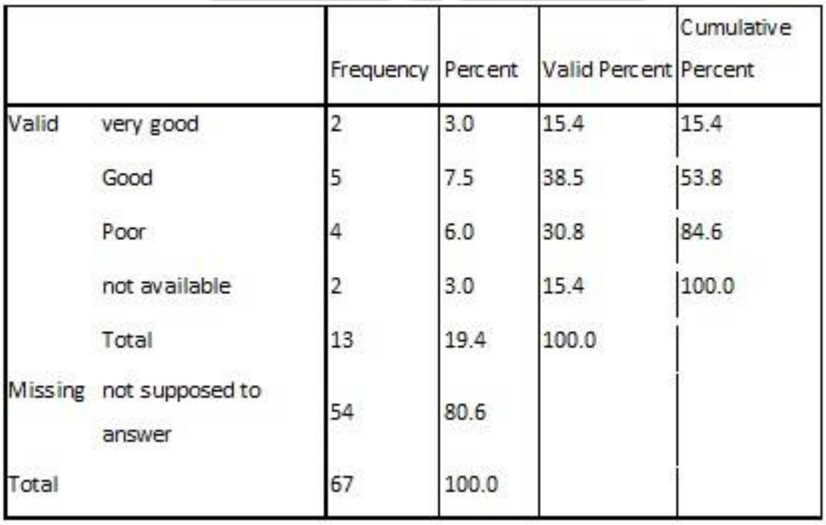
As shown in table 26, 2 of the respondents representing 3.0 % of the total population rated the reliability of WRA as being very good, 5 of the respondents representing 7.5 % of the total population rated the reliability of WRA as being good, 4 of the respondents representing 6.0 % of the total population rated the reliability of WRA as being poor and 2 of the respondents representing 3.0 % of the total population rated the reliability of WRA as not available since they did not know about its reliability.

Considering only valid responses, 2 of the respondents representing 15.4 % of the total valid responses rated the reliability of WRA as being very good, 5 of the respondents representing 38.5 % of the total valid responses rated the reliability of WRA as being good, 4 of the respondents representing 30.8 % of the total valid responses rated the reliability of WRA as being poor and 2 of the respondents representing 15.4 % of the total valid responses rated the reliability of WRA as not available since they did not know about its reliability.

From the study, majority of the respondents rated the reliability of WRA as being good.

Figure 35 illustrates the reliability of Windows Remote Assistance.

Table 26: Reliability of Windows Remote Assistance



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	very good	2	3.0	15.4	15.4
	Good	5	7.5	38.5	53.8
	Poor	4	6.0	30.8	84.6
	not available	2	3.0	15.4	100.0
	Total	13	19.4	100.0	
Missing	not supposed to answer	54	80.6		
Total		67	100.0		

Source: Field Survey, 2014

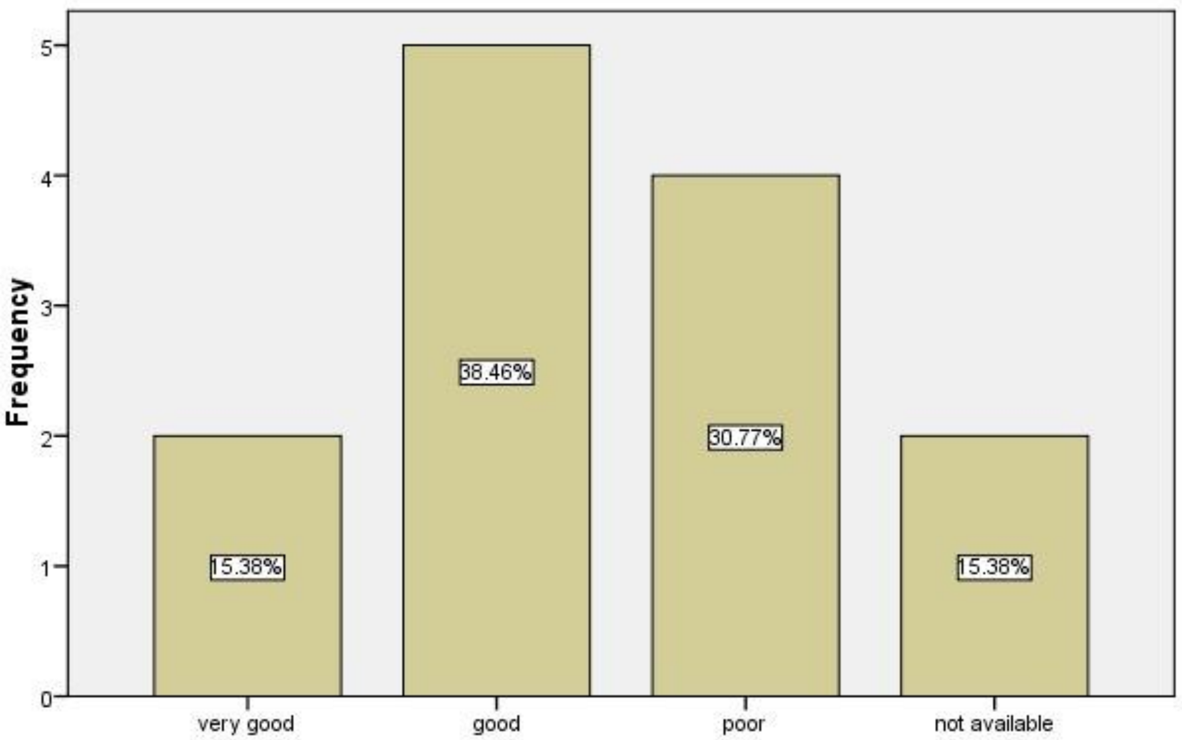


Figure 35: Reliability of Windows Remote Assistance. Source: Field Survey, 2014

4.2.25 PERFORMANCE OF WINDOWS REMOTE ASSISTANCE

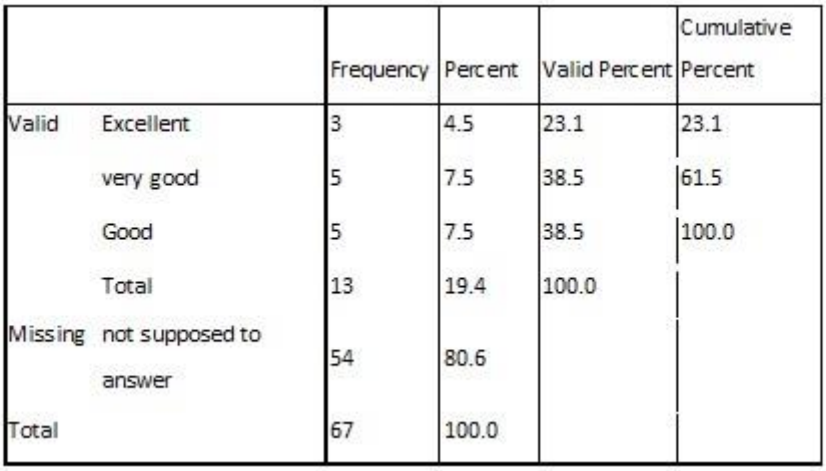
As shown in table 27, 13 of the respondents representing 19.4 % of the total population gave valid responses while 54 of the respondents representing 80.6 % of the total population did not give any response because they were not supposed to answer since they have never used WRA before.

As shown in table 27, 3 of the respondents representing 4.5 % of the total population rated the performance of WRA as being excellent, 5 of the respondents representing 7.5 % of the total population rated the performance of WRA as being very good and 5 of the respondents representing 7.5 % of the total population rated the performance of WRA as being good. Considering only valid responses, 3 of the respondents representing 23.1 % of the total valid responses rated the performance of WRA as being excellent, 5 of the respondents representing 38.5 % of the total valid responses rated the performance of WRA as being very good and 5 of the respondents representing 38.5 % of the total valid responses rated the performance of WRA as being good.

Majority of the respondents as can be seen from the study are of the view that the performance of WRA is very good and good as there is a split between the two responses.

Figure 36 is a bar chart which illustrates the performance of WRA.

Table 27: Performance of Windows Remote Assistance



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	3	4.5	23.1	23.1
	very good	5	7.5	38.5	61.5
	Good	5	7.5	38.5	100.0
	Total	13	19.4	100.0	
Missing	not supposed to answer	54	80.6		
Total		67	100.0		

Source: Field Survey, 2014

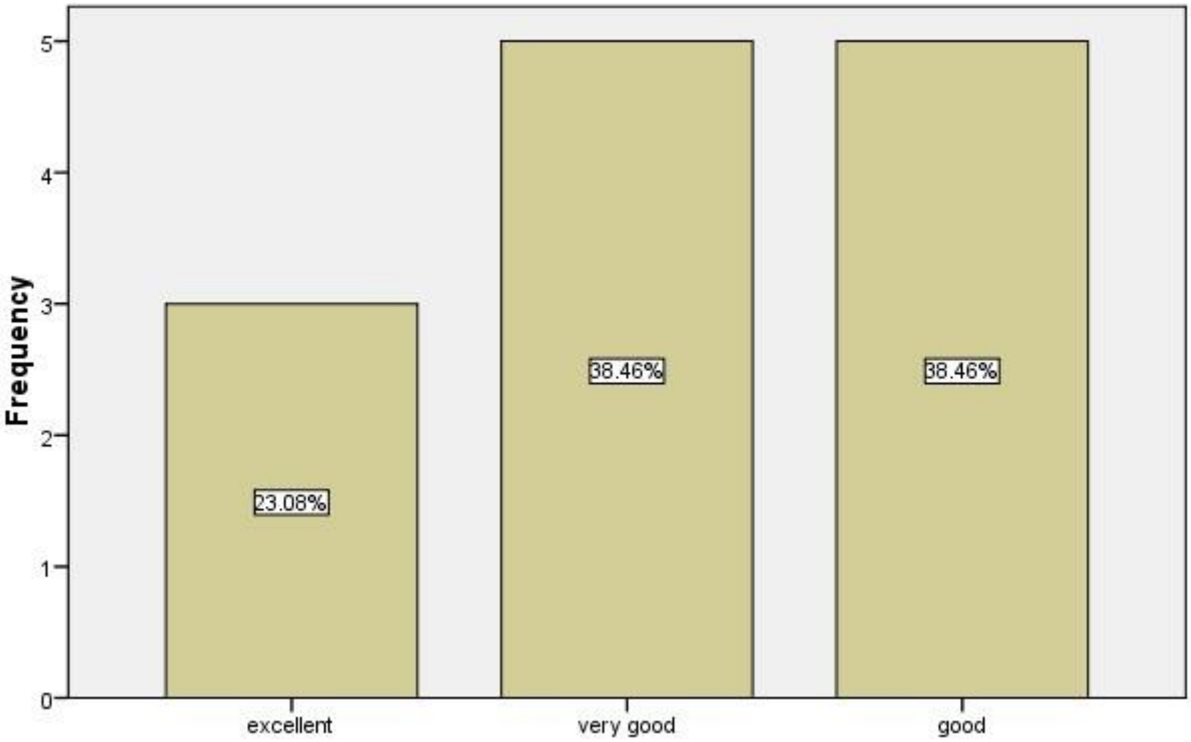


Figure 36: Performance of Windows Remote Assistance. Source: Field Survey, 2014

4.2.26 USER FRIENDLINESS OF VNC

As indicated in table 28, 11 of the respondents representing 16.4 % of the total population could rate the performance of VNC because they had used it before while 56 of the respondents, representing 83.6 % of the total population could not rate its performance because they had never used it before so were supposed to answer.

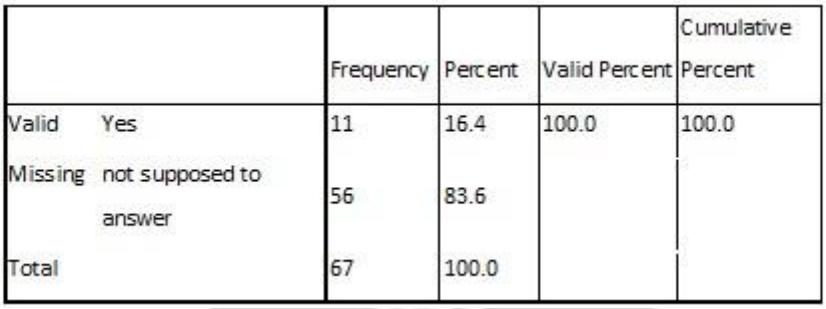
As shown in table 28 below, all 11 respondents representing 16.4 % of the total population indicated that VNC was user friendly.

For valid responses, 11 respondents representing 100.0 % of the total valid responses indicated that VNC was user friendly.

From the study, it can be concluded that VNC is user friendly since all 11 respondents agreed that it was user friendly.

Figure 37 is a bar chart which illustrates the user friendliness of VNC.

Table 28: User friendliness of VNC



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	11	16.4	100.0	100.0
Missing	not supposed to answer	56	83.6		
Total		67	100.0		

Source: Field Survey, 2014

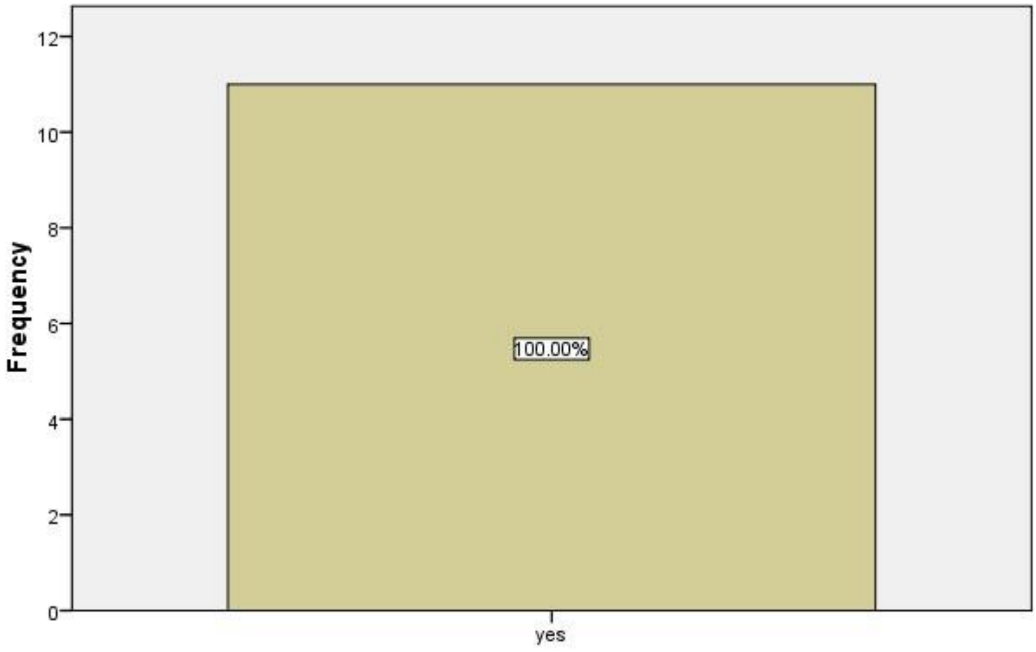


Figure 37: User friendliness of VNC. Source: Field Survey, 2014

4.2.27 USER FRIENDLINESS OF REMOTE DESKTOP

As shown in table 29 below, 38 of the respondents representing 56.7 % of the total population gave valid responses while 29 of the respondents representing 43.3 % of the total population did not indicate any response because they were not supposed to since they have never used remote desktop.

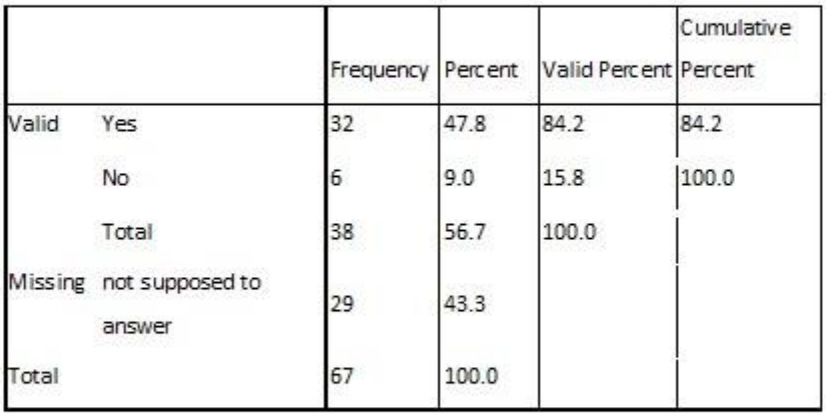
As shown in table 29, 32 of the respondents representing 47.8 % of the total population agreed that remote desktop is user friendly while 6 respondents representing 9.0 % of the total population also indicated that remote desktop was not user friendly.

Looking at only the valid responses, 32 of the respondents representing 84.2 % of the total valid responses agreed that remote desktop was user friendly while 6 of the respondents representing 15.8 % of the total valid responses agreed that remote desktop was not user friendly.

From the research findings, majority of the respondents agreed that remote desktop was user friendly.

Figure 38 is a bar chart showing the user friendliness of remote desktop.

Table 29: User friendliness of Remote Desktop



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	32	47.8	84.2	84.2
	No	6	9.0	15.8	100.0
	Total	38	56.7	100.0	
Missing	not supposed to answer	29	43.3		
Total		67	100.0		

Source: Field Survey, 2014

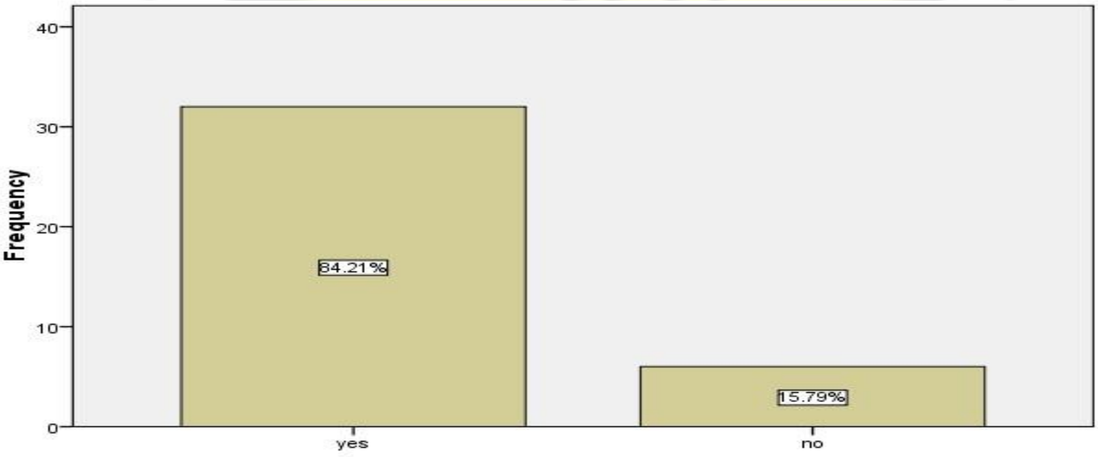


Figure 38: User friendliness of remote desktop. Source: Field Survey, 2014

4.2.28 USER FRIENDLINESS OF TEAMVIEWER

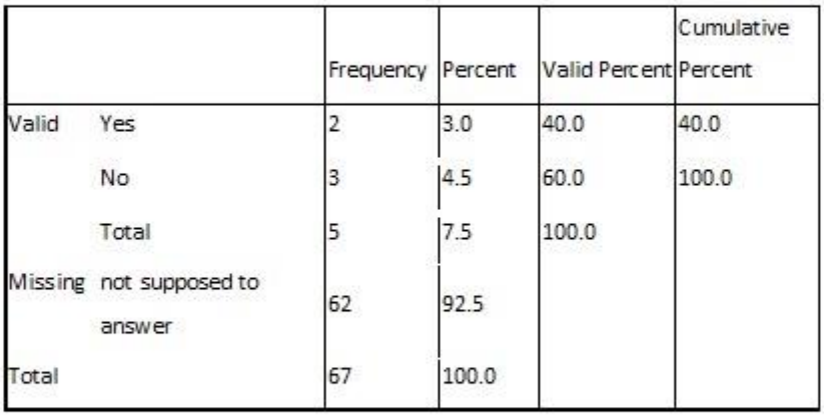
As indicated in table 30, 5 of the respondents representing 7.5 % of the total population gave valid responses while 62 of the respondents representing 92.5 % of the total population did not indicate any response because they were not supposed to answer since they had never used TeamViewer before.

Also, in table 30, 2 of the respondents representing 3.0 % of the total population agreed that TeamViewer was user friendly and 3 of the respondents representing 4.5 % of the total population agreed that TeamViewer was not user friendly.

Looking at only the valid responses, 2 of the respondents representing 40.0 % of the total valid responses agreed that TeamViewer was user friendly and 3 of the respondents representing 60.0 % of the total valid responses agreed that TeamViewer was not user friendly.

From the study, majority of the respondents agreed that TeamViewer was not user friendly. Figure 39 is a bar chart representing the user friendliness of TeamViewer.

Table 30: User friendliness of TeamViewer



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	2	3.0	40.0	40.0
	No	3	4.5	60.0	100.0
	Total	5	7.5	100.0	
Missing	not supposed to answer	62	92.5		
Total		67	100.0		

Source: Field Survey, 2014

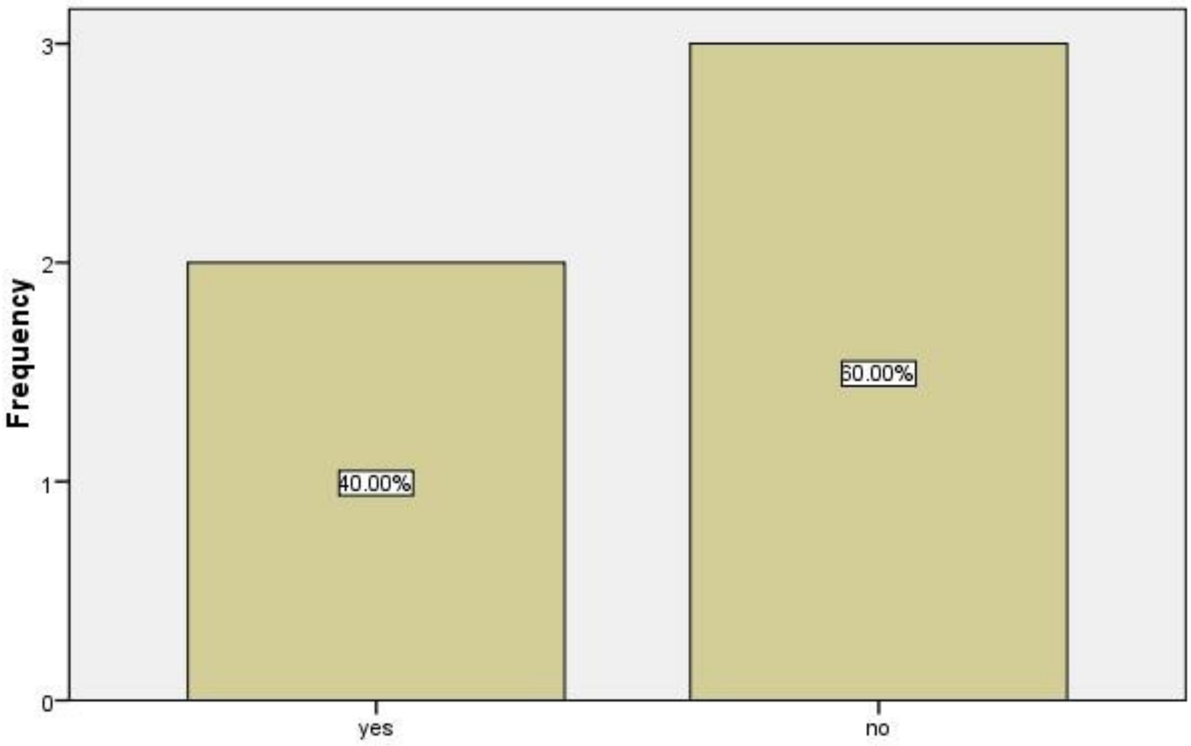


Figure 39: User friendliness of TeamViewer. Source: Field Survey, 2014

4.2.29 USER FRIENDLINESS OF WINDOWS REMOTE ASSISTANCE

As shown in table 31, 13 of the respondents representing 19.4 % of the total population gave valid responses while 54 of the respondents representing 80.6 % of the total population did not answer because they were not supposed to since they had earlier indicated they have never used WRA.

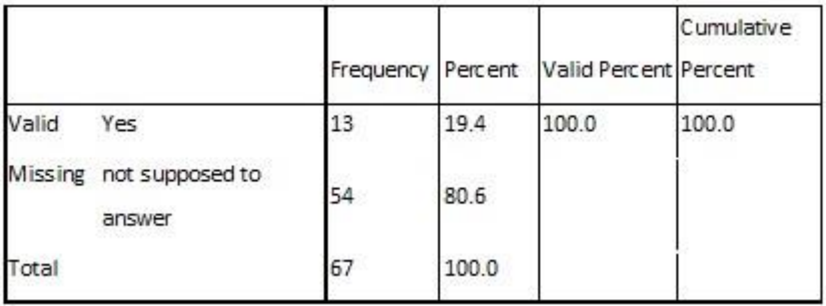
All the 13 respondents representing 19.4 % of the total population agreed that WRA was user friendly.

Considering only valid responses, all the 13 respondents representing 100.0 % of the total valid responses indicated that WRA was user friendly.

From the survey, Windows Remote Assistance is user friendly.

Figure 40 shows a bar chart representing the user friendliness of Windows Remote Assistance.

Table 31: User friendliness of Windows Remote Assistance



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	13	19.4	100.0	100.0
Missing	not supposed to answer	54	80.6		
Total		67	100.0		

Source: Field Survey, 2014

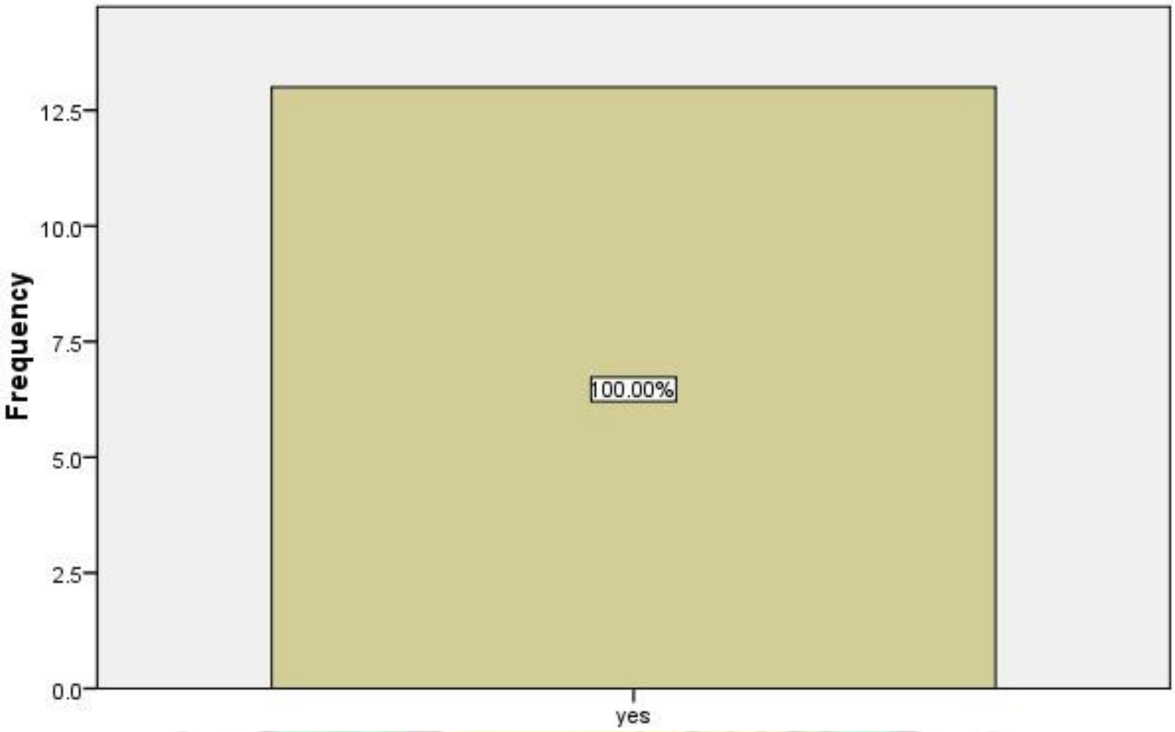


Figure 40: User friendliness of Windows Remote Assistance. Source: Field Survey, 2014

4.2.30 RESPONDENTS WHO LIKE TO SEE NEW FEATURES ADDED TO SOFTWARE

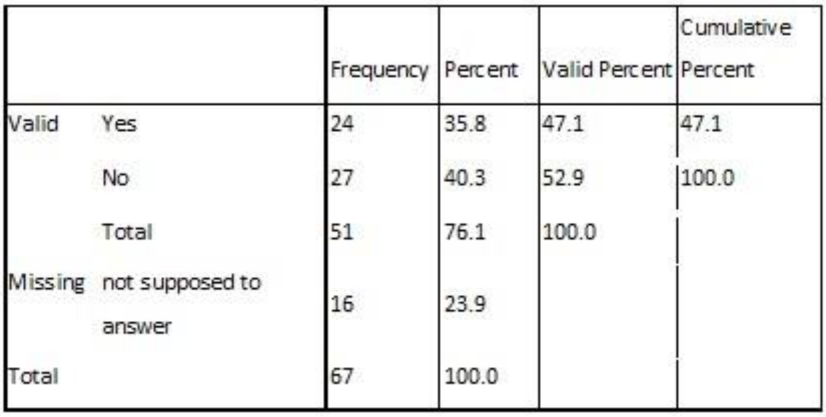
As shown in table 32, 51 of the respondents representing 76.1 % of the total population gave valid responses while 16 of the respondents representing 23.9 % of the total population did not respond because they were not supposed to once they have never used any remote software before.

Out of the 51 valid responses, 24 of the respondents representing 35.8 % of the total population indicated they wanted new features added to the software of their choice, however, 27 of the respondents representing 40.3 % of the total population indicated they did not want to see any new feature added to the software of their choice.

Looking at only the valid responses, 24 of the respondents representing 47.1 % of the total valid responses agreed that new features should be added to their choice of remote software while 27 of the respondents representing 52.9 % of the total valid responses indicated they did not want to see any new feature add to their choice of remote software. From the survey, majority of the respondents did not want to see new features add to their choice of remote software.

Figure 41 is a bar chart representing respondents' views about adding new features to their choice of remote software.

Table 32: Respondents who like to see new features added to software



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	24	35.8	47.1	47.1
	No	27	40.3	52.9	100.0
	Total	51	76.1	100.0	
Missing	not supposed to answer	16	23.9		
Total		67	100.0		

Source: Field Survey, 2014

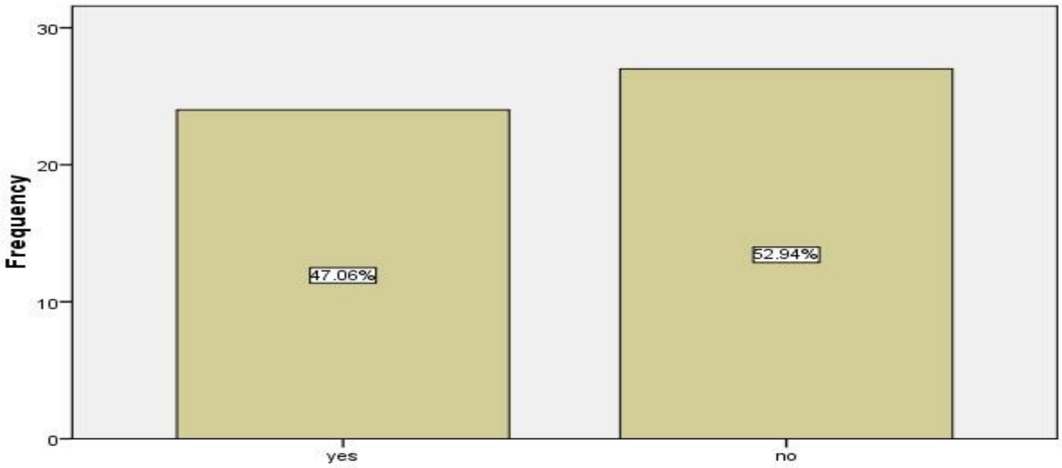


Figure 41: Respondents' views about adding new features to their choice of remote software. Source: Field Survey, 2014

4.2.31 REMOTE ACCESS SOFTWARE RESPONDENT WILL LIKE TO SEE NEW FEATURES ADDED

From table 33, 24 respondents representing 35.8 % of the total population gave valid responses by indicating the software they want new feature(s) added to while 43 of the respondents representing 64.2 % of the total population did not indicate any response because they do not see the need for any new feature to be added or they have never actually used any remote access software.

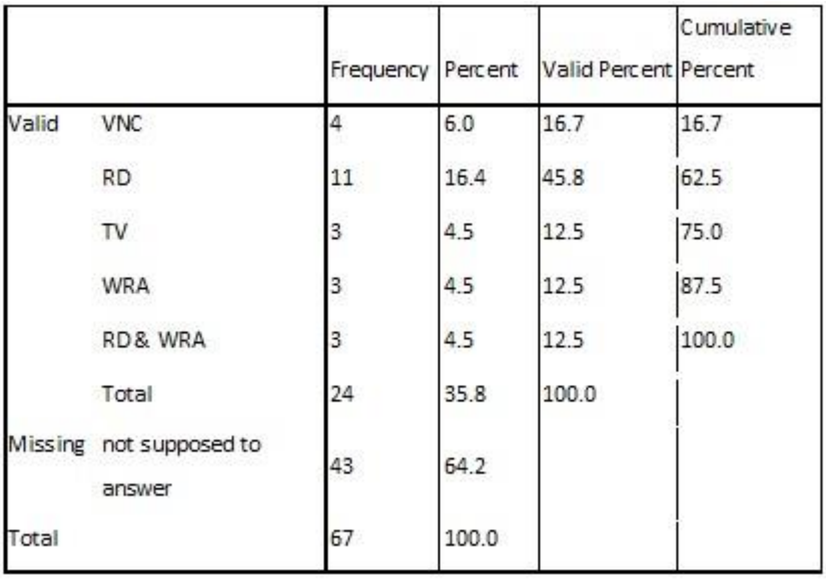
From the study, 4 of the respondents representing 6.0 % of the total population indicated they wanted new feature(s) added to VNC, 11 of the respondents representing 16.4 % of the total population indicated they wanted new feature(s) added to RD, 3 of the respondents representing 4.5 % of the total population indicated wanted new feature(s) added to TV, 3 of the respondents representing 4.5 % of the total population indicated they wanted new feature(s) added to WRA and 3 of the respondents representing 4.5 % of the total population indicated they wanted new feature(s) added to RD & WRA.

Considering only the valid responses, , 4 of the respondents representing 16.7 % of the total valid responses indicated they wanted new feature(s) added to VNC, 11 of the respondents representing 45.8 % of the total valid responses indicated they wanted new feature(s) added to RD, 3 of the respondents representing 12.5 % of the total valid responses indicated they wanted new feature(s) added to TV, 3 of the respondents representing 12.5 % of the total valid responses indicated they wanted new feature(s) added to WRA and 3 of the respondents representing 12.5 % of the total population indicated they wanted new feature(s) added to RD & WRA.

Figure 42 is bar chart illustrating remote access software respondent will like to see new features added.

From the study, it is clear that majority of the respondents indicated that they wanted new feature(s) added to RD.

Table 33: Remote access software respondent will like to see new features added



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	VNC	4	6.0	16.7	16.7
	RD	11	16.4	45.8	62.5
	TV	3	4.5	12.5	75.0
	WRA	3	4.5	12.5	87.5
	RD& WRA	3	4.5	12.5	100.0
	Total	24	35.8	100.0	
Missing	not supposed to answer	43	64.2		
Total		67	100.0		

Source: Field Survey, 2014

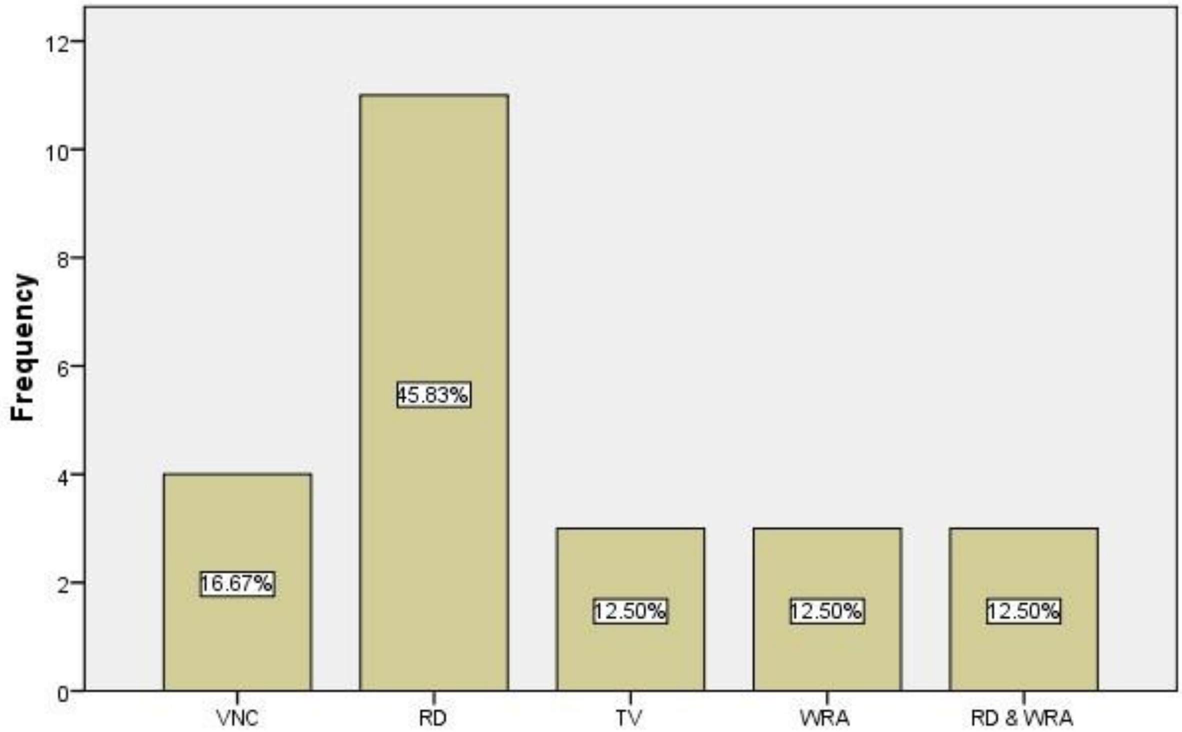


Figure 42: Remote access software respondent will like to see new features added. Source: Field Survey, 2014

4.2.32 REMOTE ACCESS SOFTWARE RESPONDENT WILL LIKE TO SEE NEW FEATURES ADDED AND NEW FEATURES RECOMMENDED BY RESPONDENT

As shown in table 34 below, 2 respondents recommended that VNC should be able to run on smartphones, 2 respondents also recommended that VNC should be able to support multi users.

Also, 7 of the respondents also indicated that RD should have improved connectivity, 2 of the respondents also indicated that RD should run on smartphones and 2 respondents also indicated that RD should be able to run on smartphones and 2 also indicated that RD should be made user friendly.

3 of the respondents also indicated that TV should be made user friendly.

3 of the respondents also recommended that WRA should be able to run on smartphones.

Also, 3 of the respondents recommended that RD & WRA should be able to support multi users.

7 respondents recommended for "**improved connectivity**", 7 respondents also recommended for "**should run on smartphones**", 5 respondents also recommended for "**should be user friendly**" and 5 respondents also recommended for "**support multi users**", so in total 24 of the total population of 67 respondents made recommendations for new features to be added to their choices of remote access software.

Figure 43 below is a bar chart representing remote access software respondent will like to see new features added and the new features recommended by the respondents.

From the survey, 35.82% of the respondents will like to see new features added to their choice of software.

Table 34: Remote access software respondent will like to see new features added and new features recommended by respondent

		new features recommended by respondent				
		improved connectivity	should run on smartphone	should be user friendly	support multi users	Total
remote access software respondent will like to see new features added	VNC	0	2	0	2	4
	RD	7	2	2	0	11
	TV	0	0	3	0	3
	WRA	0	3	0	0	3
	RD & WRA	0	0	0	3	3
Total		7	7	5	5	24

Source: Field Survey, 2014

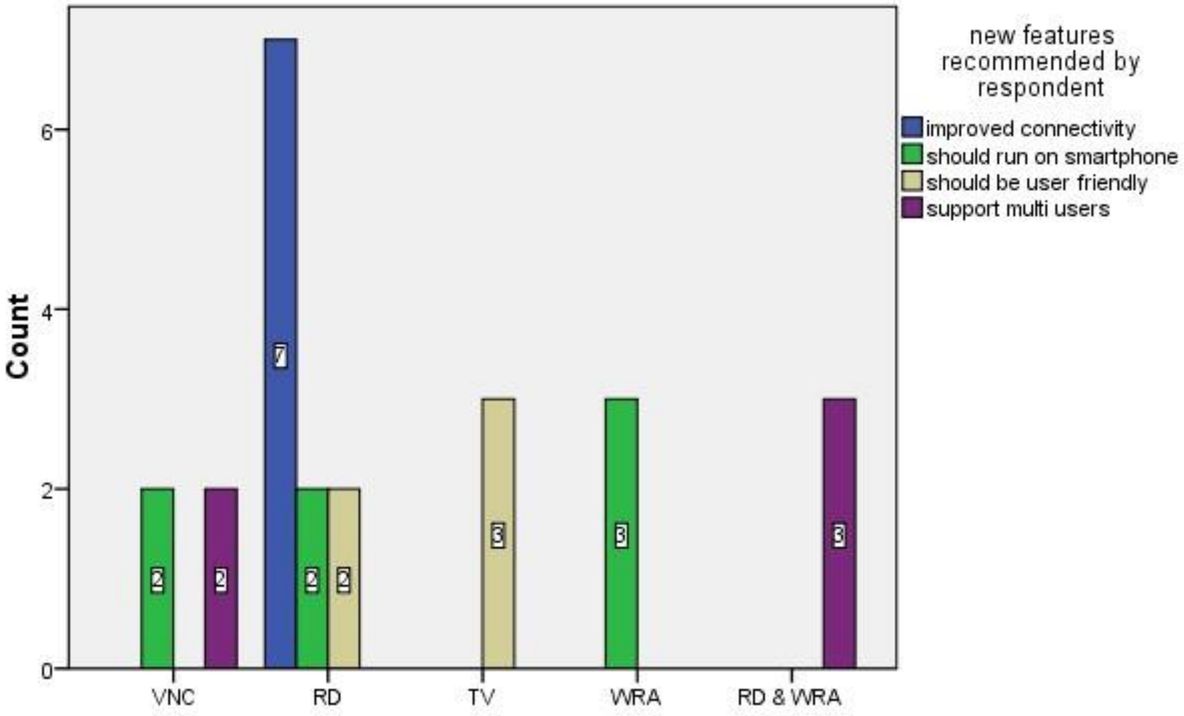
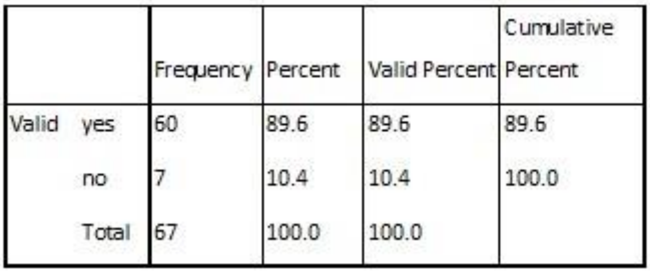


Figure 43: Remote access software respondents will like to see new features added and new features recommended by respondent. Source: Field Survey, 2014

4.2.33 ARE INNOVATIONS RELEVANT TO THE RESPONDENT?

As shown in table 35 below, out of the 67 valid responses, 60 of the respondents representing 89.6 % of the total population agreed that innovations were relevant and 7 of the respondents representing 10.4 % of the total population did not agree that innovations were relevant. From the study, majority of the respondents have agreed that innovations were relevant. Figure 44 is a bar chart representing respondents' views about innovations.

Table 35: Are innovations relevant to the respondent



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	60	89.6	89.6	89.6
	no	7	10.4	10.4	100.0
	Total	67	100.0	100.0	

Source: Field Survey, 2014

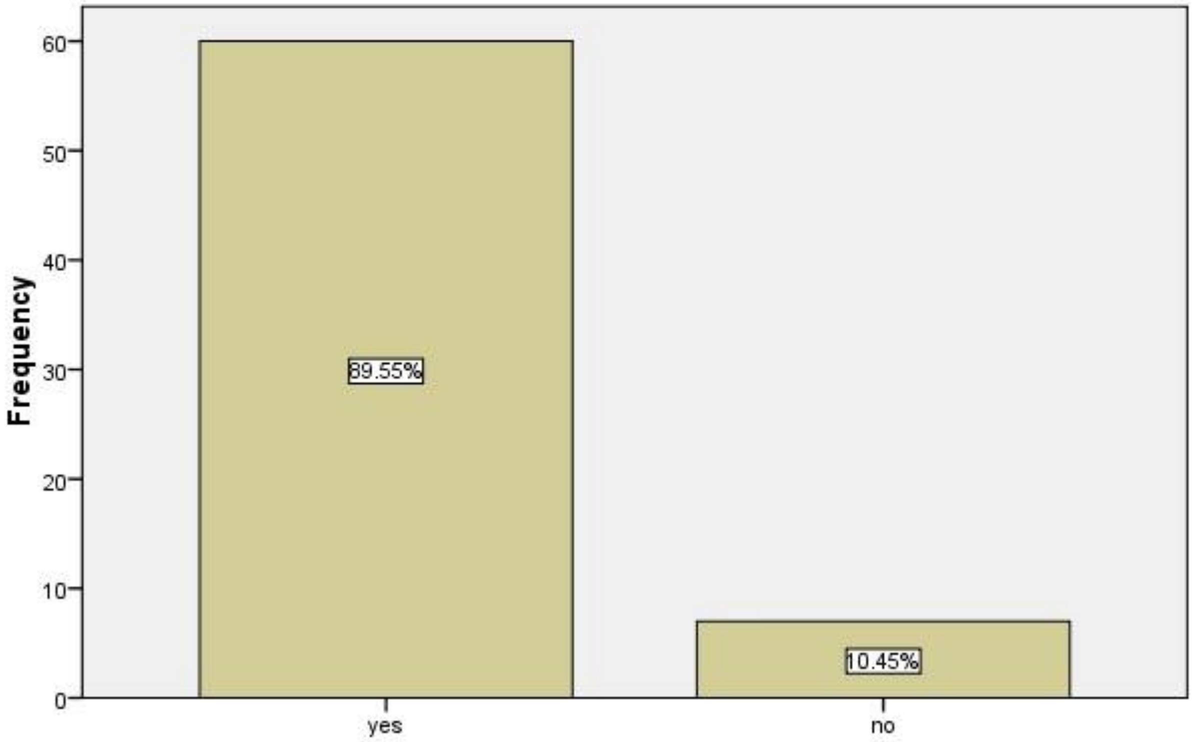


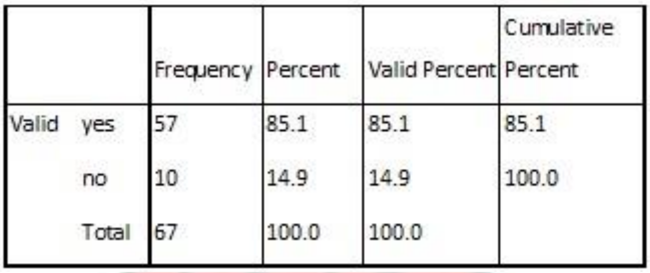
Figure 44: Respondents' views about innovations. Source: Field Survey, 2014

4.2.34 RESPONDENTS' READINESS TO ACCEPT IT INNOVATIONS

As shown in table 36, 57 of the respondents representing 85.1 % of the total population were ready to accept IT innovation while 10 of the respondents representing 14.9 % of the total population were not ready to accept IT innovation.

From the study, majority of the respondents were ready to accept IT innovations.

Figure 45 below is a chart showing respondents readiness to accept IT innovations. **Table 36: Respondents' readiness to accept IT innovations**



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	57	85.1	85.1	85.1
	no	10	14.9	14.9	100.0
	Total	67	100.0	100.0	

Source: Field Survey, 2014

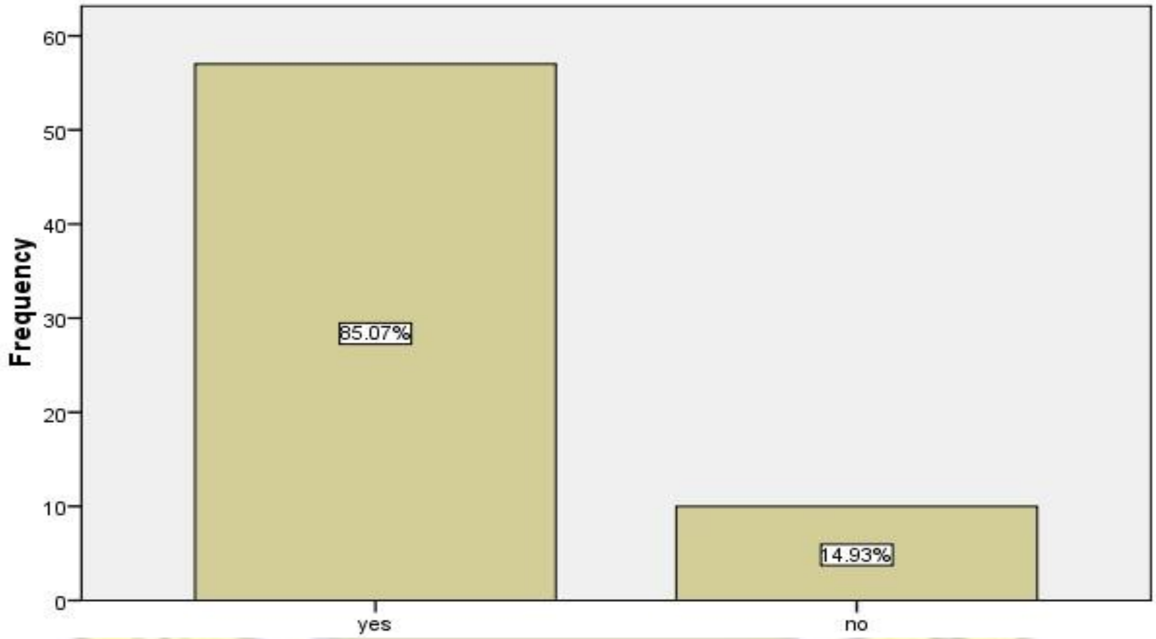


Figure 45: Respondents' readiness to accept IT innovations. Source: Field Survey, 2014

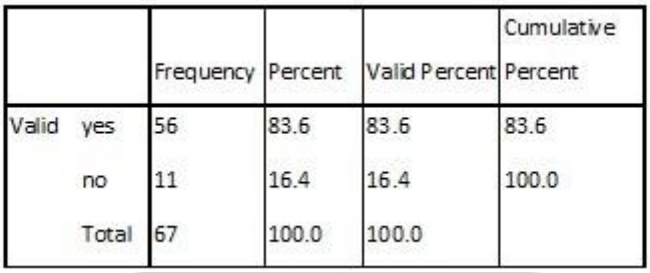
4.2.35 RESPONDENT'S READINESS TO ACCEPT A REMOTE SYSTEM ADMINISTRATION APP

As shown in table 37 56 of the respondents representing 83.6 % of the total population were ready to accept a remote system administration application that runs on smartphone, however, 11 of the respondents representing 16.4 % of the total population indicated that they were not ready to accept a remote system administration application that runs on a smartphone. One respondent who was a computer technician actually indicated he or she was not ready to accept it because it was not related to his or her work.

Figure 46 is a bar chart showing respondent's readiness to accept a remote system administration application.

From the research findings, majority of the respondents were ready to accept a remote system administration application that runs on a smartphone.

Table 37: Respondent's readiness to accept a remote system administration app



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	56	83.6	83.6	83.6
	no	11	16.4	16.4	100.0
	Total	67	100.0	100.0	

Source: Field Survey, 2014

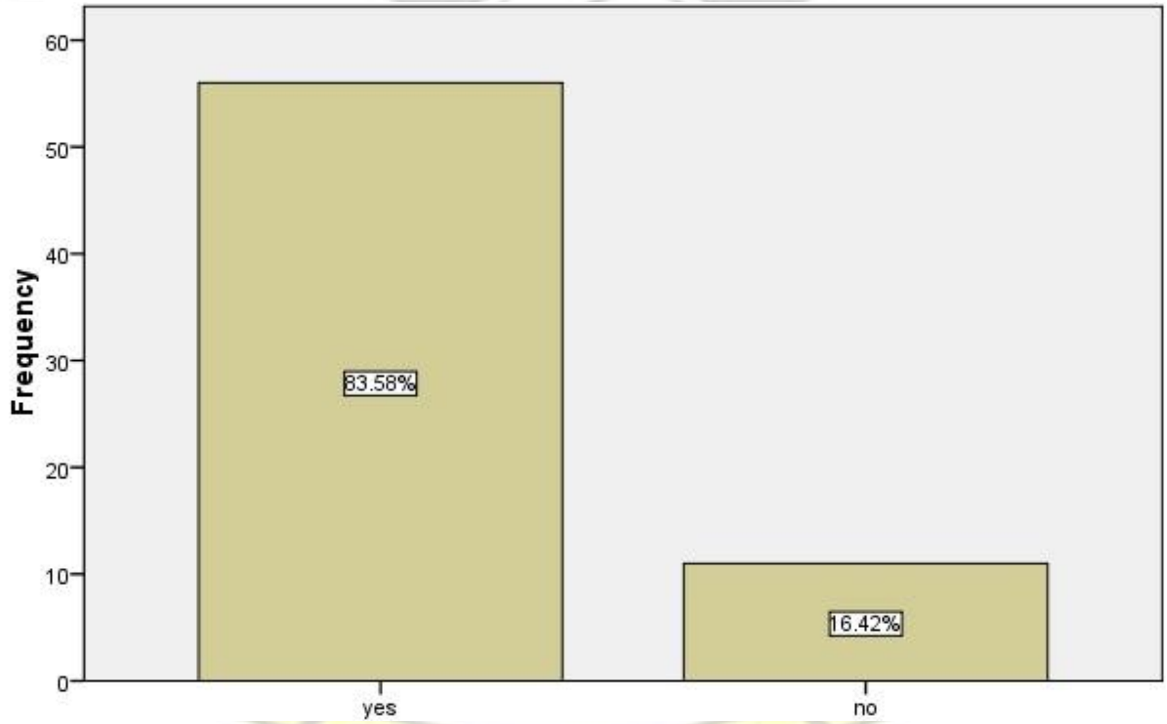


Figure 46: Respondent's readiness to accept a remote system administration app. Source: Field Survey, 2014

4.2.36 REASON FOR RESPONDENT'S ACCEPTANCE OF REMOTE ADMINISTRATION APP

As shown in table 38 below, 56 of the respondents representing 83.3 % of the total population gave valid responses while 11 of the respondents representing 16.4 % did not give any response because they were not supposed to answer since they had earlier on indicated that they will not accept a remote system administration application.

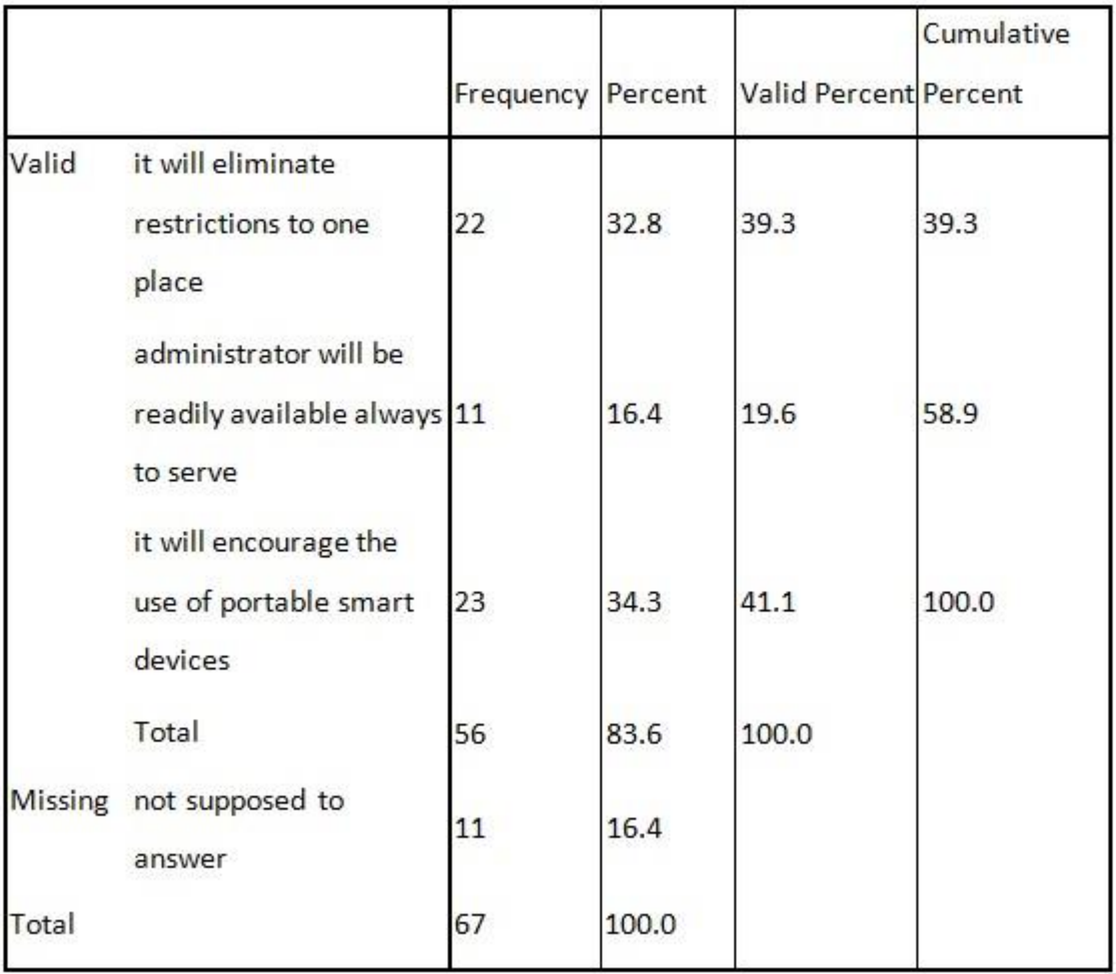
As indicated on table 38 below, 22 of the respondents representing 32.8 % of the total population indicated that they will accept a remote system administration app because it will **eliminate restrictions to one place**, 11 of the respondents representing 16.4 % of the total population indicated they will accept a remote system app because **administrator will be readily available always to serve** and 23 of the respondents representing 34.3 % of the total respondents indicated that they will accept a remote system administration app because **it will encourage the use of portable smart devices.**

Considering only the valid responses, 22 of the respondents representing 39.3 % of the total valid responses indicated that they will accept a remote system administration app **because it will eliminate restrictions to one place**, 11 of the respondents representing 19.6 % of the total valid responses indicated they will accept a remote system app because **administrator will be readily available always to serve** and 23 of the respondents representing 41.1 % of the total valid responses indicated that they will accept a remote system administration app because **it will encourage the use of portable smart devices**.

Figure 47 below is a bar chart representing reasons for respondent’s acceptance of remote system administration app.

From the study, majority of the respondents will accept a remote system app because it will encourage the use of portable smart devices.

Table 38: Reason for respondent’s acceptance of remote system administration app



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	it will eliminate restrictions to one place	22	32.8	39.3	39.3
	administrator will be readily available always to serve	11	16.4	19.6	58.9
	it will encourage the use of portable smart devices	23	34.3	41.1	100.0
	Total	56	83.6	100.0	
Missing	not supposed to answer	11	16.4		
Total		67	100.0		

Source: Field Survey, 2014

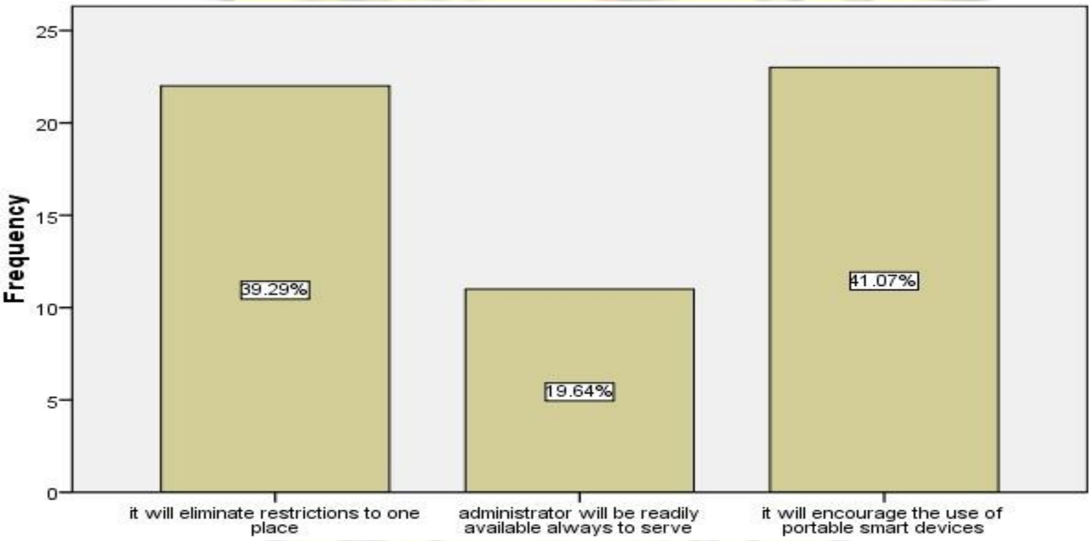


Figure 47: Reason for respondent's acceptance of remote system administration app. Source: Field Survey, 2014

4.3 SYSTEM IMPLEMENTATION, CODING AND PERFORMANCE TEST

4.3.1 USER AUTHENTICATION OR LOGIN INTERFACE

When a user starts the application, the first screen displayed on the smartphone is the login interface for the user to enter a valid user name and password. This is to ensure that only authorized users have access to the system.

The user login interface is as shown below in figure 48

Figure 48: Login interface. Source: Author's construct

4.3.2 MAIN INTERFACE

When a user successfully logs into the system, the main application interface is displayed as in figure 49 below.

On the main app interface, one can see servers and users. If a user wants to monitor a server, that server must be added first before it can be monitored. Similarly, before a user can have access to the system, that user must be added to the system before he or she can gain access to it. All these are demonstrated going forward.

From the main interface, it can be seen that the app is connected to a server named test which has an IP address of 10.0.2.2 and listening on port 80.

Figure 49: Main Interface of App. Source: Author's construct

When an administrator wants to create a user or add a user to the system, the admin must do a long tab on the users' icon on the main interface and the screen shot in figure 50 below will be displayed. The administrator can then proceed to tap New User in the menu to enter the username and password.

Similarly, an existing user can be edited by tapping Edit User in the menu, an existing user can also be deleted by tapping Delete User in the menu and a user can view a file on remote server connected to the app by tapping the View menu as shown in figure 50 below.

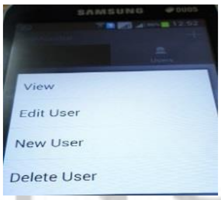


Figure 50: Menus used to perform certain actions. Source: Author's construct

Also, as shown in figure 51 below, once the app is connected to a server as in figure 49 above, files can be created and viewed on the connected server. Figure 51 below shows a PDF file on the connected sever being viewed on the app.

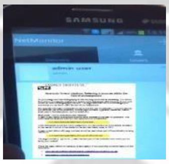
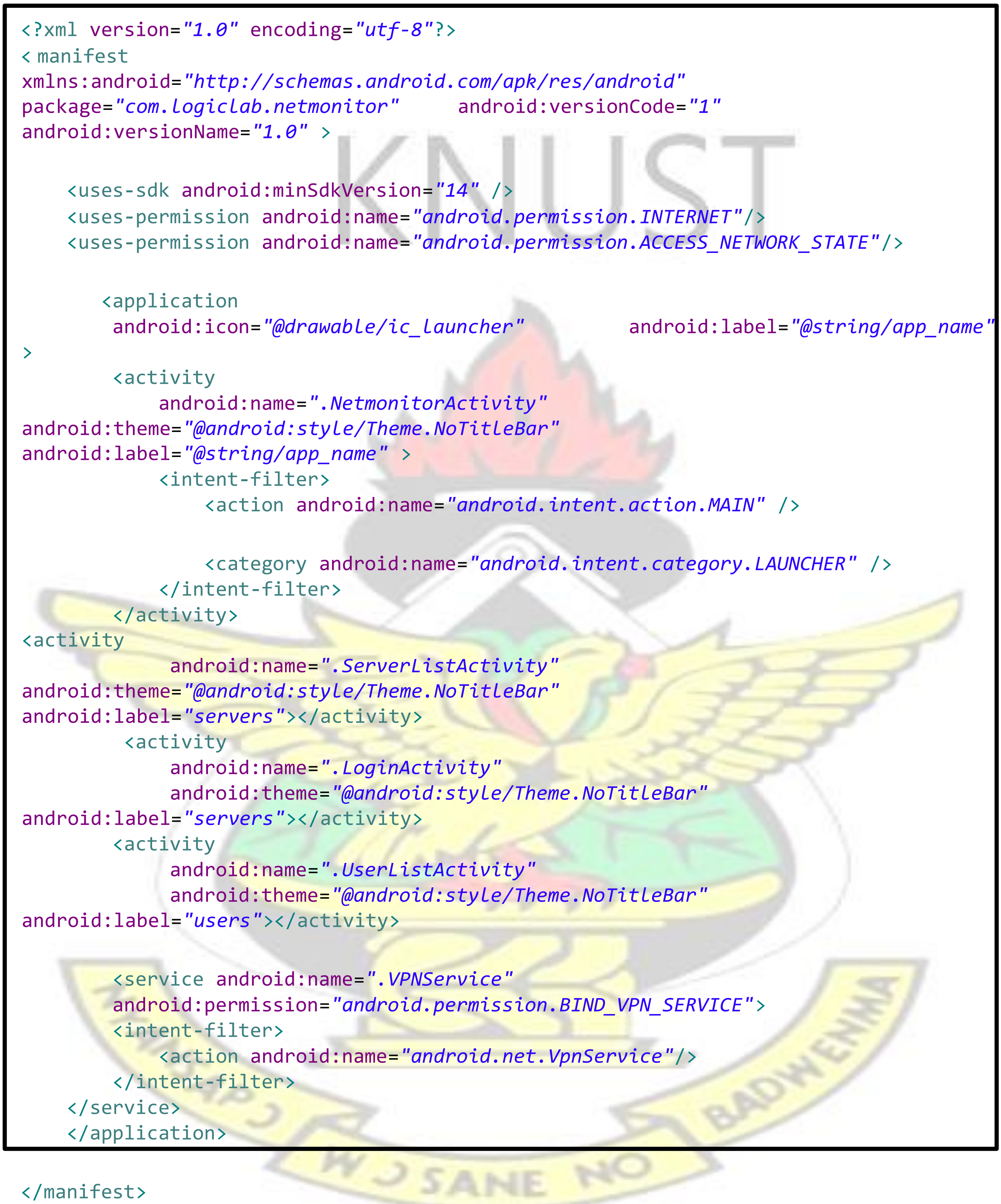


Figure 51: File on the remote server being viewed on the app by an admin. Source: Author's construct

The code snippet below is from the android manifest file.



```
<?xml version="1.0" encoding="utf-8"?>
< manifest
xmlns:android="http://schemas.android.com/apk/res/android"
package="com.logiclab.netmonitor"     android:versionCode="1"
android:versionName="1.0" >

    <uses-sdk android:minSdkVersion="14" />
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>

       <application
        android:icon="@drawable/ic_launcher"         android:label="@string/app_name"
>
        <activity
            android:name=".NetmonitorActivity"
android:theme="@android:style/Theme.NoTitleBar"
android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
<activity
             android:name=".ServerListActivity"
android:theme="@android:style/Theme.NoTitleBar"
android:label="servers"></activity>
         <activity
             android:name=".LoginActivity"
             android:theme="@android:style/Theme.NoTitleBar"
android:label="servers"></activity>
        <activity
             android:name=".UserListActivity"
             android:theme="@android:style/Theme.NoTitleBar"
android:label="users"></activity>

        <service android:name=".VPNService"
        android:permission="android.permission.BIND_VPN_SERVICE">
        <intent-filter>
            <action android:name="android.net.VpnService"/>
        </intent-filter>
    </service>
    </application>

</manifest>
```

Figure 52: Code snippet of android application. Source: Author’s construct

4.3.3 THE PROPOSED SECURE RFB PROTOCOL AND IMPLEMENTATION OF AN ANDRIOD SMARTPHONE APP FOR REMOTE SYSTEM ADMINISTRATION

In implementing the self-signed certificate in the android app, the researcher sets up a custom TrustManager that will trust the self-signed certificate this research is creating and then providing the TrustManager with the custom SSLContext as demonstrated in the code snippet shown in figure 4.42 below. This custom TrustManager is necessary to prevent the default android TrustManager not trusting the server's certificate thereby terminating connections.

This is how a self-signed certificate is created on the server the android app will be communicating with.

i. A KeyStore is created using "bcprov-jdk15on-146.jar" which is a java class. This class can be downloaded from www.bouncycastle.org/download/ bcprov-jdk15on-146.jar. This file will be stored in "C:\androidproject". This file is used to generate the KeyStore.

ii. A keytool is then used to generate the key "keytool –genkey -alias androidproject –keystore C:\androidproject/androidprojectsssl.keystore –validity 365.

iii. The above generated key is then exported from the .KeyStore file to .cer file using the command "-export –alias androidprojects –keystore C:\androidprojects\androidprojectssl.keystore –file C:\androidproject\androidprojectsslcert –cer" iv. The ".keystore file" is then saved in "/androidappdir/raw/"

v. A class called "MyAndroidClient" is then written to hardcode the self-signed generated certificate in the android app.

This class (MyAdroidClient) will load the researcher's own trust store to check the selfsigned SSL certificate instead of the android default trust store. It is only when the certificate here matches with the server that connection will be established.

The idea here is to do certificate pinning with the self-signed certificate created by the researcher by hard-coding the certificate known to be used by the server in the android app. This way, the android app will then ignore the device's (smartphone's) trust store and rely on its own and only allow SSL connections to servers with the self-signed certificate hardcoded in it.

The code snippet below is for the implementation of the self-signed SSL certificate in the android app.

```
import java.io.InputStream;
import java.security.KeyStore;

import android.content.Context;

public class MyAndroidClient extends DefaultHttpClient {

 private static Context context;

 public static void setContext(Context context) {
  MyAndroidClient.context = context;
 }

 public MyAndroidClient(HttpParams params) {
  super(params);
 }

 public MyAndroidClient(ClientConnectionManager httpConnectionManager, HttpParams params) {
  super(httpConnectionManager, params);


 @Override
    protected ClientConnectionManager createClientConnectionManager() {
        SchemeRegistry registry = new SchemeRegistry();
        registry.register(new Scheme("http", PlainSocketFactory.getSocketFactory(), 80));
        // Register for port 443 our SSLSocketFactory with our keystore
        // to the ConnectionManager
        registry.register(new Scheme("https", newSSLSocketFactory(), 443));
        return new SingleClientConnManager(getParams(), registry);
    }

    private SSLSocketFactory newSslSocketFactory() {


            // Get the raw resource, which contains the keystore with
            // your trusted certificates (root and any intermediate certs)
                    InputStream in =
        MyAndroidClient.context.getResources().openRawResource(R.raw.androidprojectssl); //name of your
        //keystore file here
            try {
                // Initialize the keystore with the provided trusted certificates
                // Provide the password of the keystore
                trusted.load(in, "g@n@@1984".toCharArray());
            } finally {
                in.close();
            }
            // Pass the keystore to the SSLSocketFactory. The factory is responsible
            // for the verification of the server certificate.
            SSLSocketFactory sf = new SSLSocketFactory(trusted);
            sf.setHostnameVerifier(SSLSocketFactory.STRICT_HOSTNAME_VERIFIER);
            return sf;
        } catch (Exception e) {
            throw new AssertionError(e);
        }
    }
}
```

}

```
        try {
```

Figure 53: Code snippet for implementing self-signed SSL certificate. Source: Author's construct

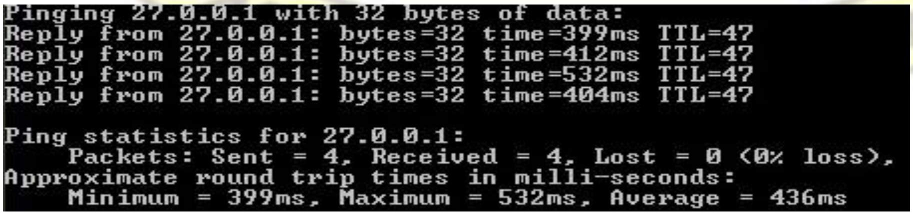
This is how the researcher implemented SSL in the android app using a self-signed SSL certificate.

4.3.4 EVALUATING THE PERFORMANCE OF THE RDP, RFB, AND THE PROPOSED SECURE RFB PROTOCOL

In undertaking the performance test of the RFB protocol, RDP protocol and the android app which is based on a secure RFB protocol, two parameters were considered. These parameters are **response time** and **availability.**

The response time of software is the time required for the software to respond to user events (Scarpino J. J., 2012).

A client was connected to a server using remote desktop which is based on the RDP protocol and the server pinged from the client and the results shown in figure 54 was obtained.



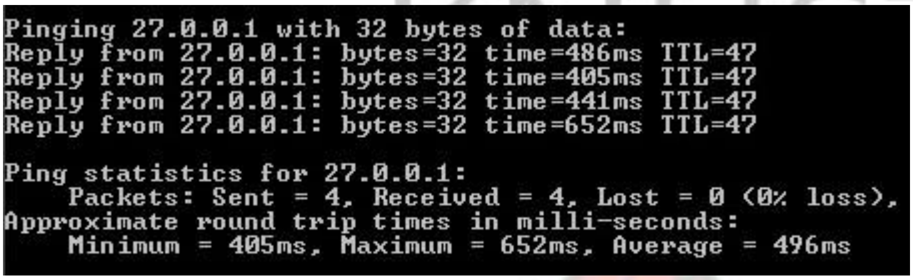
```
Pinging 27.0.0.1 with 32 bytes of data:
Reply from 27.0.0.1: bytes=32 time=399ms TTL=47
Reply from 27.0.0.1: bytes=32 time=412ms TTL=47
Reply from 27.0.0.1: bytes=32 time=532ms TTL=47
Reply from 27.0.0.1: bytes=32 time=404ms TTL=47

Ping statistics for 27.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 399ms, Maximum = 532ms, Average = 436ms
```

Figure 54: RDP ping results. Source: Source: Author's construct

From the above figure, the minimum response time from the server is 399ms, the maximum response time is 532ms and the average response time is 436ms.

Another client was connected to a server through VNC which is based on the RFB protocol and the server pinged from the client and the result shown in figure 55 was obtained.



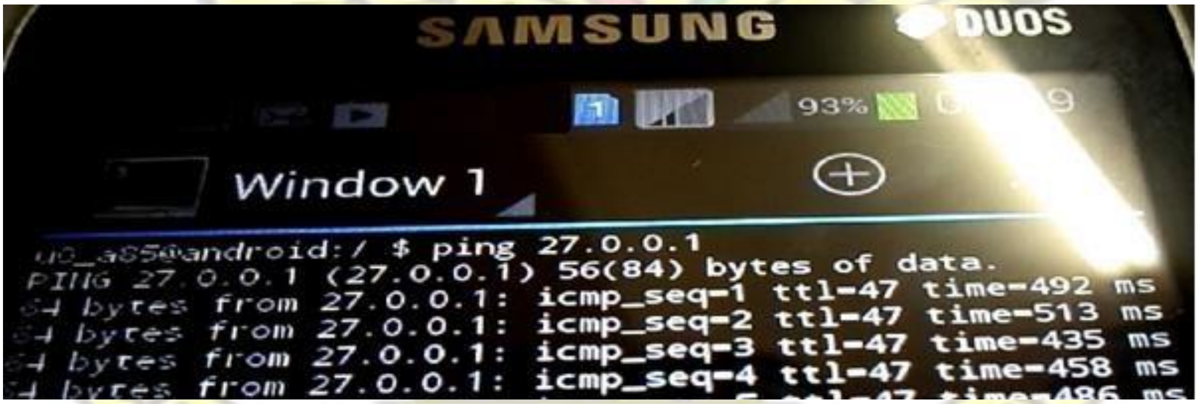
```
Pinging 27.0.0.1 with 32 bytes of data:
Reply from 27.0.0.1: bytes=32 time=486ms TTL=47
Reply from 27.0.0.1: bytes=32 time=405ms TTL=47
Reply from 27.0.0.1: bytes=32 time=441ms TTL=47
Reply from 27.0.0.1: bytes=32 time=652ms TTL=47

Ping statistics for 27.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 405ms, Maximum = 652ms, Average = 496ms
```

Figure 55: RFB ping results. Source: Author's construct

From the above figure, the minimum response time 405ms, the maximum response time is 652ms and the average response time is 496ms.

A smartphone was also connected to a server using the android app this research implemented and the server pinged from the smartphone which is the client, and the following result was obtained as shown in figure 56 below.



```
u0_a55@android:/ $ ping 27.0.0.1
PING 27.0.0.1 (27.0.0.1) 56(84) bytes of data.
64 bytes from 27.0.0.1: icmp_seq=1 ttl=47 time=492 ms
64 bytes from 27.0.0.1: icmp_seq=2 ttl=47 time=513 ms
64 bytes from 27.0.0.1: icmp_seq=3 ttl=47 time=435 ms
64 bytes from 27.0.0.1: icmp_seq=4 ttl=47 time=458 ms
64 bytes from 27.0.0.1: icmp_seq=5 ttl=47 time=486 ms
```

Figure 56: Android app (secure RFB) ping results. Source: Author's construct

From the above figure, the minimum response time is 435ms, the maximum response time is 513ms and the average response time just by calculation is 474ms.

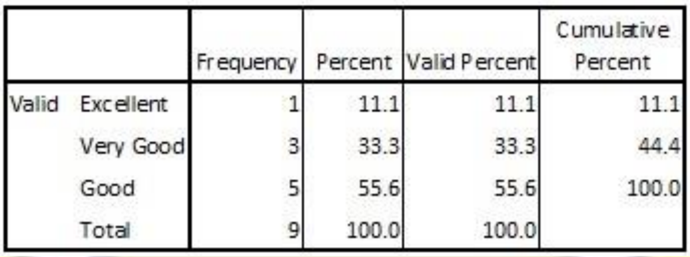
From the three figures above, one will see that, the response time of Remote Desktop (RD) which is based on the RDP protocol has an average response time of 436ms, VNC which is based on the RFB protocol has an average response time of 496ms and the android app which is based on a secure RFB protocol has an average response time of 474ms. This means that RDP has the fastest response time among the three, followed by the android app and then VNC. This confirms the statement made by (Masthan et al., 2013) that VNC applications are generally slower and offer fewer features and security options than Windows Remote Desktop.

The researcher also engaged nine (9) system administrators to use remote desktop and VNC viewer which are based on the RDP protocol and the RFB protocol respectively and also use the android app in administering their servers. After using them (RD, VNC viewer and the android app), they were required to evaluate their response times and availability through a questionnaire shown in appendix B. All the nine administrators were males and aged between 27yrs- 35yrs.

As shown in table 39 below, 1 of the respondents representing 11.1 % of the total respondents rated the response time of the android app as being excellent, 3 of the respondents representing 33.3 % of the total respondents also indicated that the response time of the app was very good and 5 of the respondents representing 55.6 % of the total responses also rated the response time of the app as good.

From the field survey, it can be concluded that the android app has a good performance **Table**

39: Performance of app in terms of response time



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	1	11.1	11.1	11.1
	Very Good	3	33.3	33.3	44.4
	Good	5	55.6	55.6	100.0
	Total	9	100.0	100.0	

Source: Field Survey, 2014

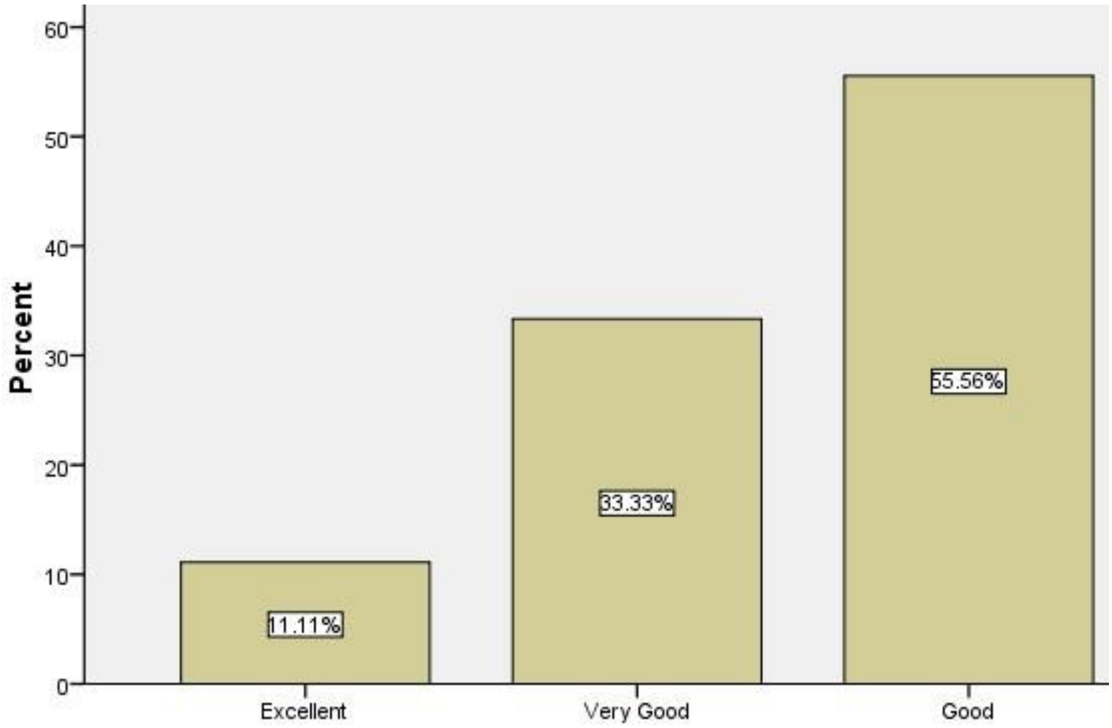
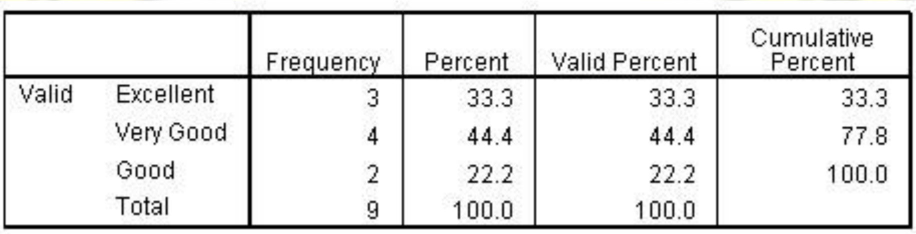


Figure 57: Performance of android app in terms of response time. Source: Field Survey, 2014

As shown in table 40 below, 3 of the 9 respondents representing 33.3 % rated the availability of the android app as being excellent, 4 of the 9 respondents representing 44.4 % indicated that the availability of the app was very good and 3 of the 9 respondents representing 22.2 % indicated that the availability of app was good.

Figure 58 below is a bar chart representing the views of the nine respondents on the availability of the android app.
From the field survey, the availability of the android app is good.

Table 40: Availability of android app



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	3	33.3	33.3	33.3
	Very Good	4	44.4	44.4	77.8
	Good	2	22.2	22.2	100.0
	Total	9	100.0	100.0	

Source: Field Survey, 2014

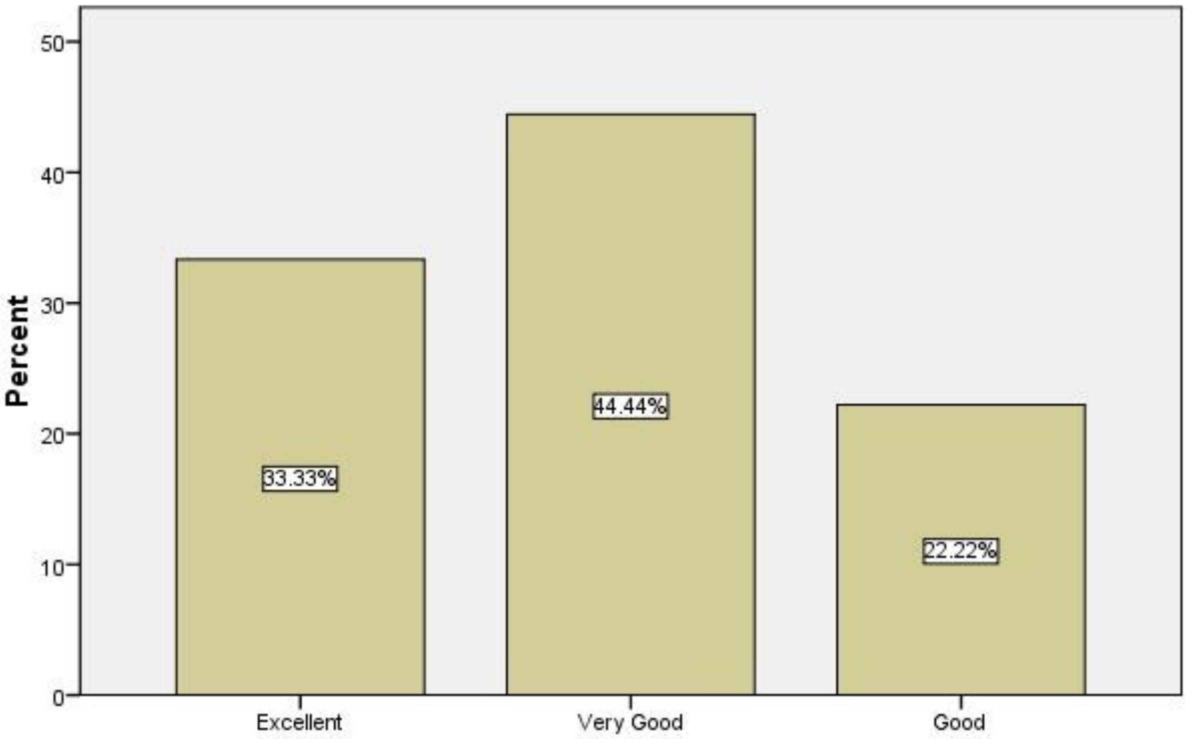
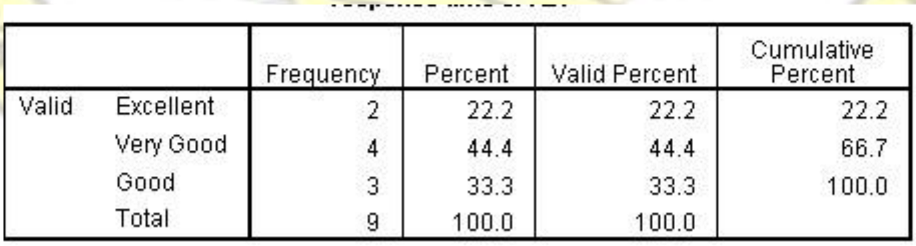


Figure 58: Availability of android app. Source: Field Survey, 2014

As shown in table 41 below, 2 of the respondents representing 22.3 % of the total respondents rated the response time of the RDP protocol as excellent, 4 of the respondents representing 44.4 % of the total respondents also rated its response time as very good and 3 of the respondents representing 33.3 % of the total respondents rated its response time as good.

Figure 59 below is a bar chart representing the response time of the RDP protocol.

Table 41: Performance of RDP in terms of response time



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	2	22.2	22.2	22.2
	Very Good	4	44.4	44.4	66.7
	Good	3	33.3	33.3	100.0
	Total	9	100.0	100.0	

Source: Field Survey, 2014

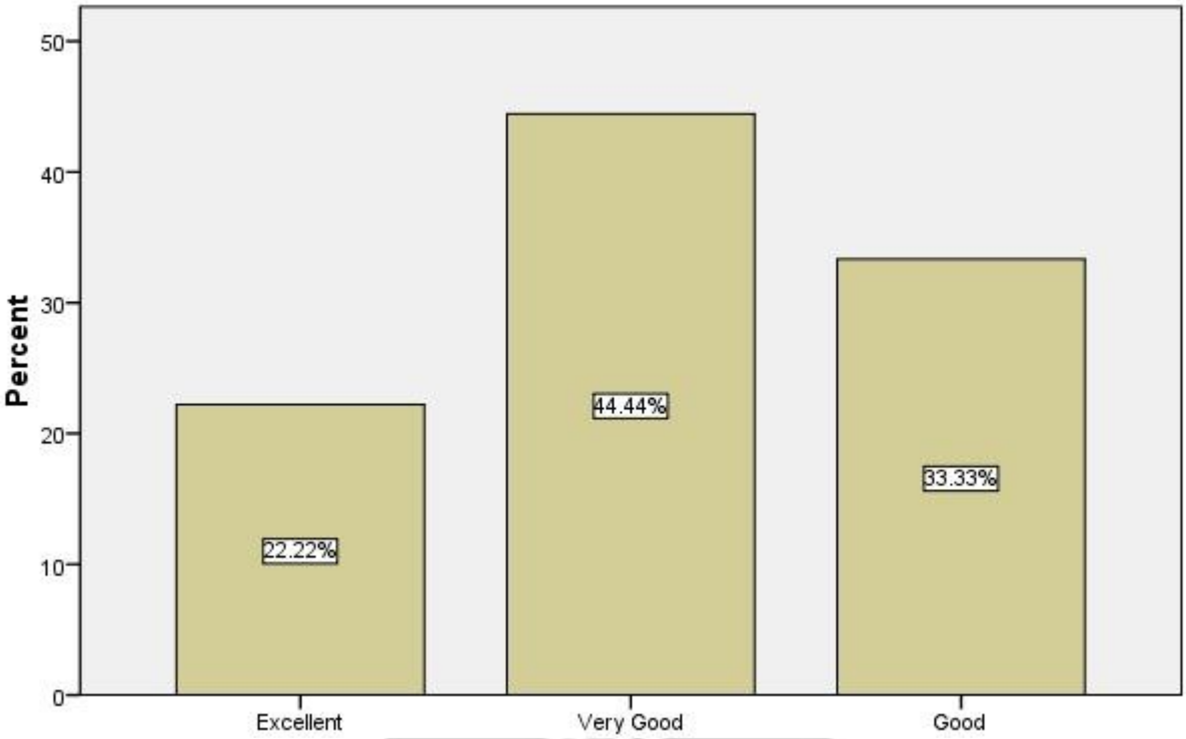
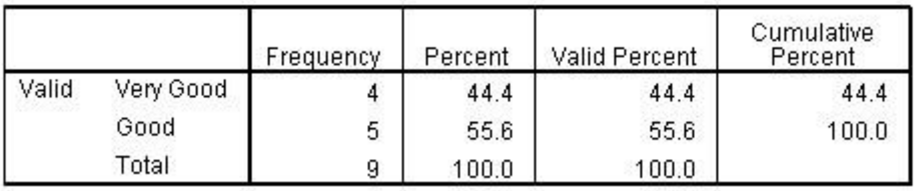


Figure 59: Performance of the RDP protocol in terms of response time. Source: Field Survey, 2014

As indicated in table 42 below, 4 of the 9 respondents representing 44.4 % rated the availability of the RDP protocol as very good and 5 of the 9 respondents representing 55.6 % rated its availability as good.

Figure 60 below is a chart representing the availability of the RDP protocol.

Table 42: Availability of RDP protocol



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Good	4	44.4	44.4	44.4
	Good	5	55.6	55.6	100.0
	Total	9	100.0	100.0	

Source: Field Survey, 2014

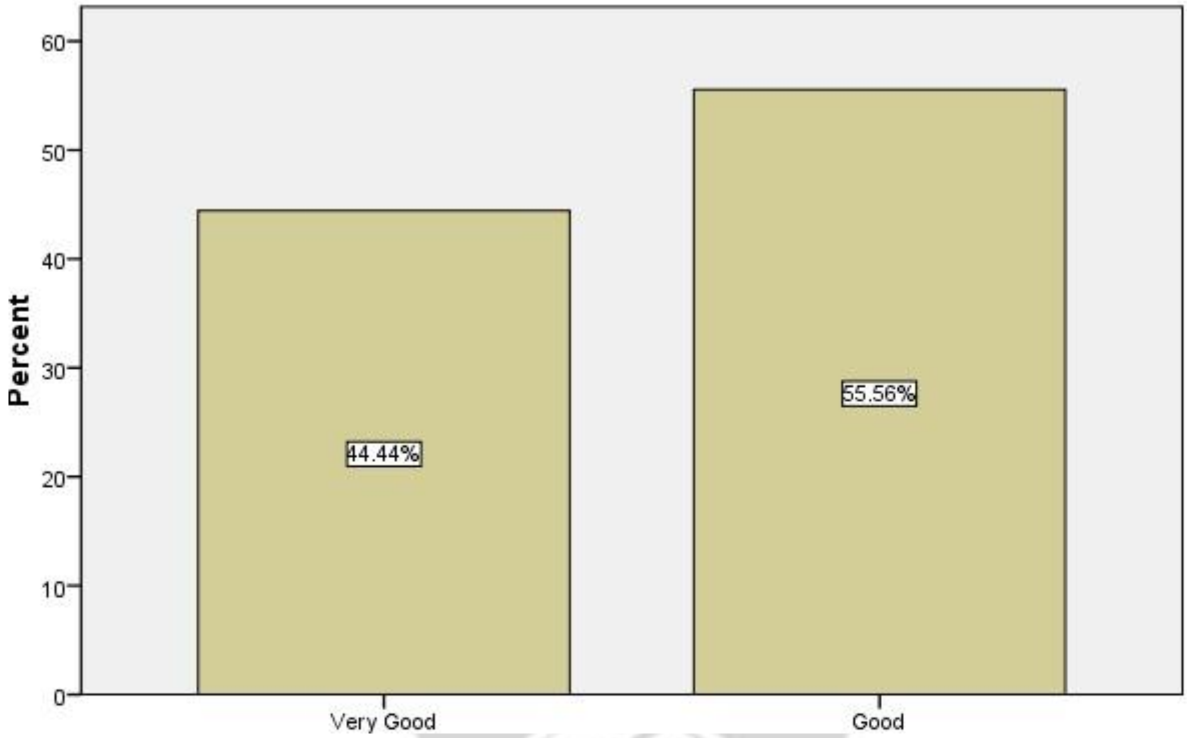
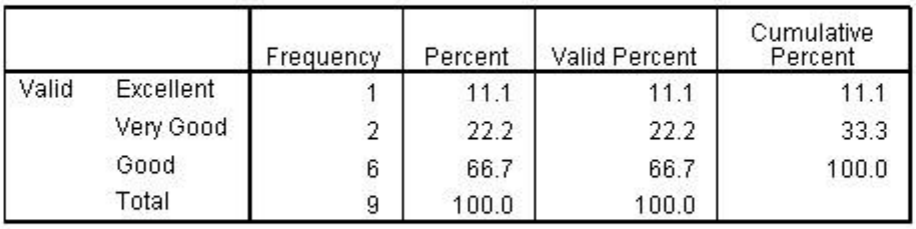


Figure 60: Availability of RDP protocol. Source: Field Survey, 2014

As shown in table 43 below, 1 of the 9 respondents representing 11.1 % rated the response time of the RFB protocol as excellent, 2 of the 9 respondents representing 22.2 % rated the response time as very good and 6 of the 9 respondents representing 66.7 % rated the response time as good.

Figure 61 below is a chart representing the response time of the RFB protocol.

Table 43: Performance of RFB protocol in terms of response time



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Excellent	1	11.1	11.1	11.1
	Very Good	2	22.2	22.2	33.3
	Good	6	66.7	66.7	100.0
	Total	9	100.0	100.0	

Source: Field Survey, 2014

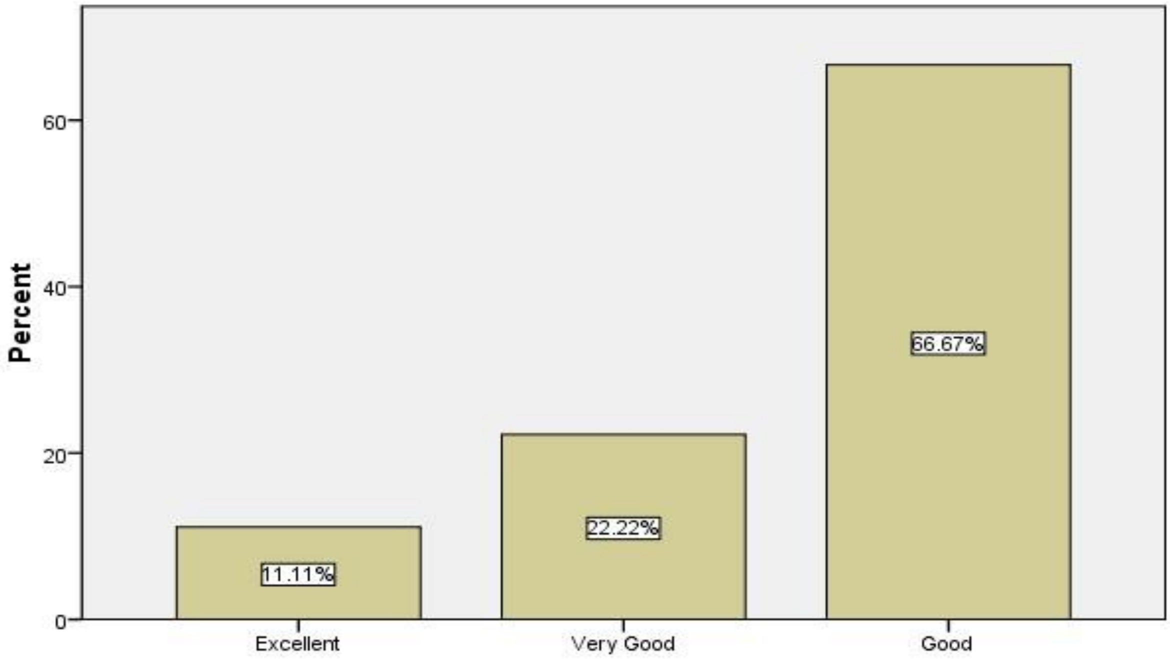
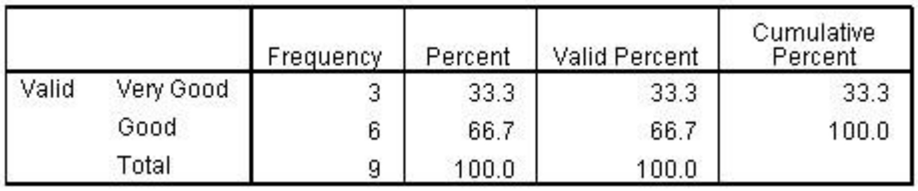


Figure 61: Performance of RFB protocol in terms of response time. Source: Field Survey, 2014

As indicated in table 44 below, 3 of the 9 respondents representing 33.3 % indicated that the availability of the RFB protocol (VNC) was very good and 6 of the 9 respondents representing 66.7 % indicated that it was good.

Figure 62 below is a chart representing the availability of the RFB protocol (VNC).

Table 44: Availability of RFB protocol (VNC)



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Good	3	33.3	33.3	33.3
	Good	6	66.7	66.7	100.0
	Total	9	100.0	100.0	

Source: Field Survey, 2014

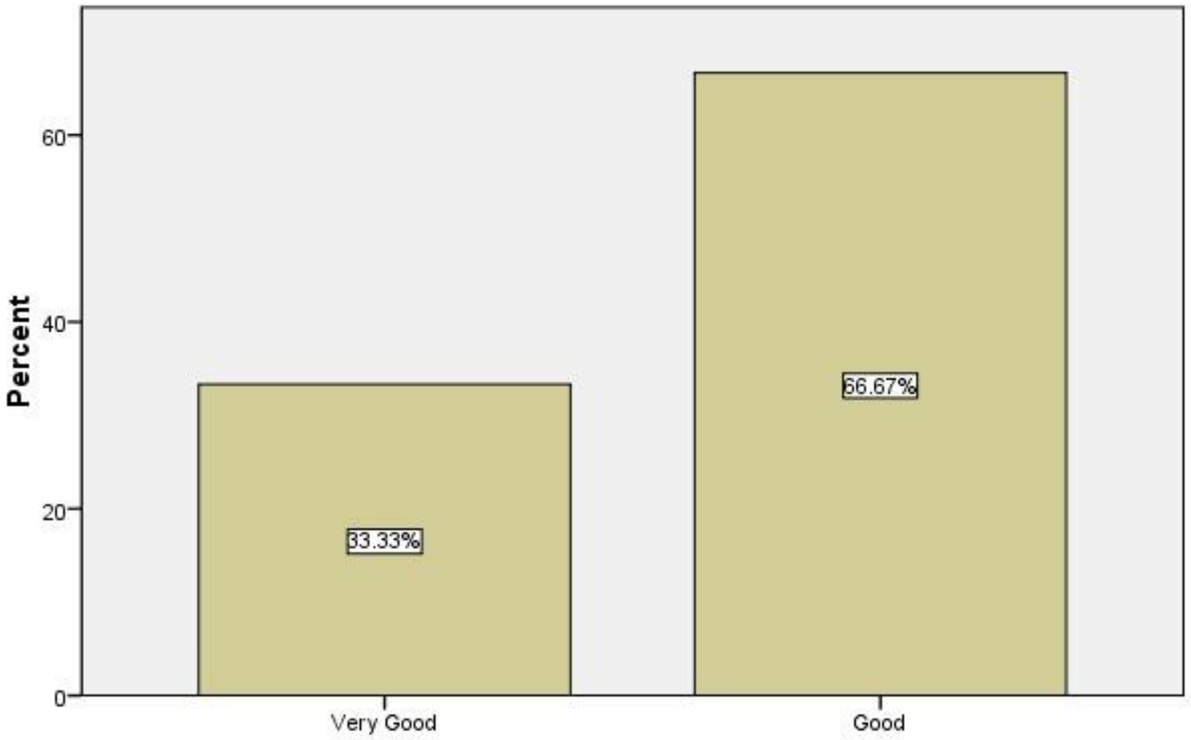


Figure 62: Availability of RFB protocol (VNC app). Source: Field Survey, 2014

From the performance test, it was realised that the RDP protocol (Remote Desktop) has the fastest response time, followed by the android app which is based on a secure RFB protocol and then RFB protocol (VNC) has the slowest response time amongst the three. It is worth noting that this does not deviate from the responses received from the 9 system administrators engaged to evaluate the RDP protocol (Remote Desktop), the RFB protocol (VNC) and the android app based on a secure RFB protocol. 22.2 % of the respondents rated the response time of the RDP protocol as excellent, whilst 11.11 % of the respondents rated the response time of the RFB as excellent and 11.11 % also rated the response time of the app which is based on a secure RFB protocol as excellent.

For the availability of the RDP protocol, the RFB protocol and the android app, 33.3 % of the respondents rated the availability of the android app as excellent while no respondent rated the availability of the RDP or the RFB protocols as excellent, making the android app more available than the other two. One of the respondents actually stated that the only time the android app is not available is when there is no network service on the mobile phone it is running on. The researcher again wishes to state that, this evaluation is true since the android app cannot run offline as stated in the constraints in chapter 3. Also, the android app runs on a portable device as compared to the RDP protocol (Remote Desktop) and RFB protocol (VNC) which run on only desktop and laptop computers.

4.4 SUMMARY

The chapter analysed (interpreted) all the responses obtained through the questionnaires administered using Statistical Package for Social Sciences (SPSS) version 17. Data coding was also done using SPSS 17 before even the data entry could commerce leading to the subsequent data analysis.

From the performance test conducted, the average response time of the RDP protocol was 436ms, that of the RFB protocol was 496ms and that of the android app which is based on a secure RFB protocol was 474ms. Also, 33.3 % of the respondents rated the availability of the android app as excellent while no respondent rated the availability of the RDP or the RFB protocols as excellent. This makes the android app more available than the other two since it runs on a very portable device which is easily carried along with user.

Implementation of self-signed SSL certificate was also carried out in this chapter to make sure connections between client and server are secured.

Some screen shots of the android app which were taken during the testing stages were also included in this chapter.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

This chapter summarizes the contributions of this research and recommends some areas for future study to be conducted on.

5.2 SUMMARY

This research has been able to prove that:

i. From the performance evaluation, the average response time of the RDP protocol (Remote Desktop) was 436ms, the average response time of the RFB protocol (VNC) was 496ms and the average response time of the android app which is based on a secure RFB protocol was 474ms. This means that if a user connects to a remote server through remote desktop and issues a command from the remote desktop client to the remote desktop server, the user will get response from the remote desktop server in 436 milliseconds. In the same way, for the RFB protocol (VNC), the user will get response from the VNC server in 496 milliseconds and for the secure RFB protocol (android app), the user will get response from the server in 474 milliseconds. This means the RDP protocol has the fastest response time and closely followed by the secure RFB protocol (android app).

ii. Also, from the performance evaluation, the android app was rated by respondents as being more available than the RDP and RFB protocols as 33.33 % of respondents' rated the availability of the android app as excellent as against no respondent rating the availability of the other two as excellent.

iii. The study revealed that 25.37% of the respondents use remote access software for virtual desktop (a user's desktop that comes from a server), 31.34% of the respondents use remote access software for file transfer, 23.88% of the respondents use remote access software for accessing terminal servers and 19.40% of the respondents use remote access software for providing assistance. This means that majority of the respondents (System Administrators) use remote access software to transfer files from one computer to another.

iv. From the study, it was established from the literature review that in terms of security, the RDP protocol is more secure than the RFB protocol.

v. It is also possible to view files on a remote computer using a smartphone.

vi. Though RFB and RDP are both remote access protocols, RFB places very little processing demands on its clients and hence is a very suitable protocol for developing applications that may run on phones or thin clients whiles RDP places much processing demands on its clients and hence a very suitable protocol for developing applications that may run on clients with high processing abilities.

vii. System administrators were very willing to accept a remote system administration app that will run on smartphones.

5.3 CONCLUSION

This research work has been able to demonstrate beyond reasonable doubt that it is very practical to deploy a system on a smartphone that can be used to support network administrators and other related professionals in their line of work to dramatically improve the services they provide to their clients or people who patronise the services they provide.

Conclusively, the research work has been able to provide an effective and productive network service delivery for network administrators.

The study revealed that some of the available remote access technologies are the Remote Frame Buffer (RFB) protocol and the Remote Desktop (RDP) protocol.

A survey involving 67 network administrators carried out by this study to find out how they are using remote access software revealed that 51 of the respondents representing 76.12% have actually used remote access software in their line of duty and the remaining 16 respondents representing 23.88% have never used remote accessed software in their line of duty.

Out of the 51 network administrators who have used remote access software in their line of duty, 19.60% of the respondents use remote access software for virtual desktop, 33.3% of the respondents use remote access software for file transfer, 23.50% of the respondents use remote access software for accessing terminal servers and 23.50% of the respondents use remote access software for providing assistance.

From the study, it was revealed through literature that by default the data that travels through the terminal server and client in the case of the RDP protocol is protected by the RC4 symmetric encryption algorithm which provides 3 levels of security. It was further revealed through literature that applications based on RFB protocol offer fewer features and security options than remote desktop which is based on the RDP protocol.

This research revealed that the average response time of the RDP protocol (Remote Desktop) was 436ms, the average response time of the RFB protocol (VNC) was 496ms and the average response time of the android app which is based on a secure RFB protocol was 474ms.

The research has also been able to establish that applications based on the RDP protocol are generally faster or give quick responses than those based on the RFB protocol from the performance test conducted by this research backed by some literature.

What this research is adding to knowledge is successfully addressing the security lapses identified in the RFB protocol used to develop the android app by incorporating self-signed Secure Socket Layer (SSL) certificate into the app to ensure that a secure connection is always established between the server and the android app in order to fight Man-In-TheMiddle (MITM) attacks.

Furthermore, from the literature review, remote access software which is based on RFB protocol places very little demand on RFB clients as opposed to those which are based on RDP which places all processing demands on RDP clients. Because remote access software based on RFB places very little demand on RFB clients, it can slow than server response which is not so in the case of those based on RDP.

From the research, the researcher has observed that, though both RFB and RDP are remote access protocols, RFB is intended to be used to develop remote access software that will run on thin clients and mobile phones which have less processing power such as low CPU speed and low memory, however, RDP is intended to be used to develop remote access software that will run on computers that have more processing power like high CPU speed and high memory.

Finally, the adoption of the product of this research work when deployed in monitoring computer networks offers a good contribution to network administration which ensures that network administrators take their networks along with them in their smartphones anywhere they go.

5.4 RECOMMENDATIONS

Apart from the two remote access technologies (RDP and RFB) that this research work looked at, in the future, other remote protocols like the Point-to-Point Protocol (PPP) which came up in the course of administering the questionnaires can be researched into.

It is also recommended that in the future the android app be made to be able to monitor and administer at least two remote servers at a time.

The researcher also recommends that in the future a huge barrier will be broken if the app could be developed to run offline, that is even when there is no internet service on the smartphone it is installed on.

It is also recommended that, in the future, modifications could be made to the app so that when a user wants to use it to connect to a server for monitoring purposes, the user is required to enter only the servers name and IP address instead of the server’s name, IP address and port number as currently done when connecting to a server to monitor it.

REFERENCES

1. Ahamed S.S.R (2009) Studying the feasibility and importance of software testing: an analysis. *International Journal of Engineering Science and Technology*. Volume 3. pp. 119. [Accessed: 3rd February, 2015)
2. Baig S, Rajasekar M. & Balaji P. (2012) Virtual Network Computing Based Remote Desktop Access. *International Journal of Computer Science and Telecommunications.* Volume 3, Issue 5. pp. 127. [Accessed: 6th June, 2014]

3. Behboodian N. & Razak S. A. (2011) ARP Poisoning Attack Detection and Protection in WLAN via Client Web Browser. *International Conference on Emerging Trends in Computer and Image Processing*. pp. 20. [Accessed:15th March, 2014]

4. BigFix Inc. (2007) Remote Desktop for Windows. pp. 2. Retrieved from: http://support.bigfix.com/product/documents/BigFixRemoteDesktopGuide-v1.pdf. [Accessed: 21st July, 2014]

5. Boling D. (2007) Windows Embedded CE 6.0 R2 Remote Desktop Protocols and Internet Explorer. pp. 6. Retrieved from: http://download.microsoft.com/download/5/8/e/58e0c008-fc15-4a3b-9728c0103bab6473/Windows%20Embedded%20CE%206.0%20R2%20Remote%20Deskto p%20Protocol%20and%20Internet%20Explorer whitepaper.pdf. [Accessed: 10th August, 2014]

6. Burgess F. T (2001) A general introduction to the design of questionnaires and for survey research. pp. 1. Retrieved from: http://iss.leeds.ac.uk/downloads/top2.pdf. [Accessed: 8th August, 2014]

7. Chauhan A, Reecha R. S, Sangeeta A, Saurabh K. & Sharma S. (2011) SMS based Remote Control System. *International Journal of Computer Science and Management Studies*. Volume 11. (Issue 2). pp. 19. [Accessed: 22nd March, 2014]

8. Chintalapati B, J. & Srinivasa R. T. Y. S. (2012) Remote computer access through Android mobiles. *International Journal of Computer Science Issues.* Volume 9. (Number 3). pp. 363. [Accessed: 10th March, 2014]

9. Code Project (2014) Android Security-Implementation of Self-Signed SSL Certificate for your App. Retrieved from:

www.codeproject.com/articles/826045/androidsecurity-implementation-of-self-signed-SSL. [Accessed: 29th January, 2015].

10. Dvorski, D. D. (2007) Installing, Configuring, and Developing with XAMPP. pp. 1. Retrieved from: www.dalibor.dvorski.net [Accessed: 4th June, 2014]

11. Entrust Incorporation. (2007) *Understanding Digital Certificates & Secure Socket Layer.* pp. 4. Retrieved from: www.entrust.com. [Accessed: 6th February, 2015]

12. Fall R. K, & Stevens R. W. (2011) TCP/IP Illustrated. . 2nd Edition. PUBLISHER: Vervante. [Online] Poughkeepsie-New York. pp. 585. Retrieved from: www.redbooks.ibm.com/redbooks. [Accessed: 12th May, 2014]

13. Georgiv M, Iyenga S, Jana S, Anubhai R, Boneh D & Shmatikov V (2012) The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software. pp. 1. Retrieved from: www.dl.acm.org. [Accessed: 4th February, 2015]

14. Groš S. (2011) Security Risk Assessment of TeamViewer Application. pp. 1. Retrieved from: http://www.zemris.fer.hr/~sgros/publications/conferences/iti2011.pdf [Accessed: 3rd March, 2014]

15. Inamdar I. A, Aggarwal H, Kadam S. & Kadhane M. (2013) COMPDROID -Remote Desktop Access through Android Mobile Phone. *International Journal of Innovative Science and Modern Engineering.* Volume 2. (Issue 1). pp. 25-26. [Accessed: 4th April, 2014]

16. Kerai P. (2010) Tracing VNC and RDP Protocol Artefacts on Windows Mobile and Windows Smartphone for Forensic Purpose. *In Proceedings of International Cyber Resilience Conference.* Australia. pp. 58. Retrieved from: http://ro.ecu.edu.au/icr/7

[Accessed: 20th March, 2014]

17. Lahaie C. (2013) TeamViewer Forensics. pp. 3. Retrieved from: www.champlain.edu/Documents/LCDI/.../Team-Viewer-Forensics.pdf. [Accessed: 13th September, 2015]

18. LogMeIn Inc. (2013) *Form 10-K Annual Report.* USA. pp. 1. Available from: http://public.thecorporatelibrary.net/Annual/AR_2012_171249.pdf. [Accessed: 8th January, 2014]

19. Masthan K, Kumar S. K. & Prasad H. V. (2013) Virtual Network Computing of User Appliances. International Journal of Computer Science and Mobile Computing. Volume 2, Issue 8. pp. 132. [Accessed: 10th September, 2014]

20. Mathew S. & Jacob P. (2008) Use of Novel Algorithms MAJE4 and MACJER-320 for Achieving Confidentiality and Message Authentication in SSL & TLS. *World Academy of Science, Engineering and Technology*. Volume 2. pp. 339. [Accessed: 4th February, 2015]

21. Montoro M. (2005) Remote Desktop Protocol, the Good, the Bad and the Ugly. pp. 1-2. Available from: www.oxid.it. [Accessed: 8th April]

22. Morris V. (2008) *Remote Desktop Tutorial.* pp. 2. Retrieved from: www.ginnymorris.com. [Accessed: 3rd January, 2014]

23. Munassar, N. M. A. & Govardhan, A. (2010) A Comparison between Five Models of Software Engineering. *International Journal of Computer Science Issues.* Volume 7. (Issue 5). pp. 95. [Accessed: 25th June, 2014]

24. Naidoo P. (2011) Intercultural Communication: A Comparative Study of Japanese and South African Work Practice. PhD Thesis, University of Zululand-South Africa. pp. 113. Retrieved from : http://uzspace.uzulu.ac.za/bitstream/handle/10530/593/PHD%20Thesis%202011_Paulene%20Naidoo.pdf?sequence=1 . [Accessed: 12th April, 2014]

25. Nam Y. S, Jurayev S, Kim S, Choi K. & Choi S. G (2012) Mitigating ARP poisoning-base man-in-the-middle attacks in wired or wireless LAN. *EURASIP Journal on Wireless Communication and Networking.* pp. 2. [Accessed: 11th February, 2015]

26. Parziale L, Britt T. D, Davis C, Jason, Forrester W, Liu W, Mathews C. & Rosselot N. (2006) *TCP/IP Tutorial and Technical Overview.* 8th Edition. PUBLISHER: Vervante. Poughkeepsie-New York. pp. 1. Retrieved from: www.redbooks.ibm.com/redbooks. [Accessed: 12th April, 2014]

27. Richardson T, Stafford-Fraser Q, Wood R, K & Hopper A. (1998) *Virtual Network Computing.* pp. 34. Retrieved from: www.qandr.org. [Accessed:28th February, 2014]

28. Richardson T. (2010) *The RFB Protocol*. pp. 3. Retrieved from: www.realvnc.com. [Accessed: 10th April, 2014]

29. Roosa S. B. & Schultze S. (2010) The “Certificate Authority” Trust Model for SSL: A Defective Foundation for Encrypted Web Traffic and a Legal Quagmire. *Intellectual Property & Technology Law Journal.* Volume 22, Number 11. pp. 3. [Accessed: 4th February, 2015]

30. Samprati S. (2012) Next Generation of Internet Protocol for TCP/IP Protocol Suite. *International Journal of Scientific and Research Publications.* Volume 2, Issue 6. pp. 1. [Accessed: 8th April, 2014]

31. Scarpino J.J (2012) Evaluating and Implementing Load Performance Testing Tools to Test Adobe Flex and Other Rich Internet Application: A Case Study. *Issues in Information Systems*. Volume 13, Issue 1. pp. 3. [Accessed: 4th February, 2015]

32. Sommerville I. (2009) Software Engineering. 9th Edition. Publisher: Pearson Education, Inc. pp. 126. Retrieved from: http://www.SoftwareEngineering-9.com. [Accessed: 5th April, 2015]

33. VNC User Guide (2012) Version 5.0. pp 49. Retrieved from: https://www.realvnc.com/products/vnc/documentation/5.0/guides/user/VNC_User_Guide.pdf. [Accessed: 10th June, 2014]

34. Wegmann, A. & Genilloud, G (2000) *The Role of "*Roles*"* in Use Case Diagrams*.* pp. 1. Retrieved from: http://dscwww.epfl.ch. [Accessed: 10th June, 2014]

35. XAMPP (2015) Download available from: www.apachefriends.org/en/xamppwindows.html. [Accessed: 16th May, 2015]

36. Yang Y. & Li L. (2012) Turn Smartphones into Computer Remote Controllers. *International Journal of Computer Theory and Engineering.* Volume 4. (Number 4). pp. 562. [Accessed: 10th March, 2014]

37. Youming L. (2013) *Virtual Networking for Mobile Cloud Computing*. Master's Thesis, Aalto University-Finland. pp. 19. Retrieved from: https://into.aalto.fi/download/attachment/.../Lin_Youming_thesis.pdf? [Accessed: 10th April, 2014]

APPENDICES

APPENDIX A

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY-KUMASI

GHANA

INSTITUTE OF DISTANCE LEARNING (IDL)

QUESTIONNAIRE

Introduction

I am a student from the Computer Science Department of Kwame Nkrumah University of Science and Technology, currently undertaking a study on “A comparative study of Remote Access Technologies and proposed implementation of a smartphone app for remote system administration”.

I humbly plead with you to share your sincere and candid knowledge with me through this questionnaire to provide me with good and relevant findings. Information you provide here is solely for academic purpose and would be treated with strict confidentiality. Thank you very much for your time.

Instructions:

In this questionnaire, boxes and spaces are provided for responses. Please tick in the appropriate box or write on the spaces.

1. What is your Gender? (a) Male [ ] (b) Female [ ]
2. What is your Age?

   (a) 21- 30 years [ ]

   (b) 31-40 years [ ]

   (c) 41- 50 years [ ] (d) 51 years and above [ ]
3. What is your Occupation?

   (a) Network/System Administrator [ ]

   (b) Computer Technician [ ]

   (c) Other

   Specify……
4. Have you ever used remote access software to carry out your duties?

   (a) Yes [ ] (b) No [ ]
5. If YES to question 4 above, what do you usually use the remote access software for?

   (a) Providing Assistance [ ] (b) Virtual Desktop [ ] (c) File Transfer [ ]

   (d) Other specify…………………………………………………………………………………………………
6. If YES to question 4 above, how long have you been using remote access software?

   (a) 6 - 10 years [ ] (b) 1 - 5 years [ ] S (c) less than a year [ ] (d) Not before [ ]
7. Do you have any knowledge about the protocols/technologies used in developing remote access software? (a) Yes [ ] (b) No [ ]
8. Which remote access technology/protocol do you have knowledge about? Tick all that is applicable

   (a) Remote Frame Buffer (RFB) [ ]

   (b) Remote desktop protocol (RDP) [ ]

(c) Other specify ………………………………………………………………………………………………..

9. How informed are you about your choice in question 7 above?

   (a) High knowledge [ ]

   (b) Moderate knowledge [ ]

   (c) Low knowledge [ ] (d) No knowledge [ ]

10. Which remote access software have you probably used in your line of work before? Tick whichever is applicable.

   (a) Virtual Network Computing (VNC) [ ]

   (b) Remote Desktop (RD) [ ]

   (c) TeamViewer [ ]

   (d) Others specify ……………………………………………………………………………………………….

11. What inspires you to continually use your choice above?

   (a) User friendly [ ]

   (b) Adequate security of connection [ ]

   (c) Reliability [ ]

   (d) Performs well [ ]

   (e) Other specify ………………………………………………………………………………………….

12. Do you know the protocol/technology your choice of remote access software in question 10 above is built on?

   (a) Yes [ ]   (b) No [ ]

13. If yes to question 11, with reference to question 9, which technology/protocol is the software of your choice based on? Tick all that is applicable

   (a) Remote frame buffer [ ]

   (b) Remote desktop protocol [ ]

   (c) Other specify ………………………………………………………………………………………….

With reference to the technology/protocol used by your choice of software, rate questions 13-15 on a scale of 1 – 4 (i.e. 1- Excellent, 2 - Very Good, 3 – Good, 4 – Poor, 5- not available).

14. How do you rate the efficiency of the software?

	1	2	3	4	5

Virtual Network Computing (VNC)					
Remote Desktop (RD)					
TeamViewer					
Others					

15. How do you rate the reliability of the software?

	1	2	3	4	5
Virtual Network Computing (VNC)					
Remote Desktop (RD)					
TeamViewer					
Other					

16. How do you rate the performance of the software?

	1	2	3	4	5
Virtual Network Computing (VNC)					
Remote Desktop (RD)					
TeamViewer					
Others					

17. Is the software (your answer) in question 9 above user friendly? Tick Yes or No against the applicable software you chose in question 9 above

	Yes	No
Virtual Network Computing (VNC)		
Remote Desktop (RD)		

TeamViewer		
Others		

18. Would you like to see any new feature(s) added to any of the remote access software you have used before? (a) Yes [ ] (b) No [ ]

19. If yes, which of the remote access software will you like to see new feature(s) added to? Tick all that is applicable

	Tick
Virtual Network Computing (VNC)	
Remote Desktop (RD)	
TeamViewer	
Others	

20. What new feature(s) will you like to see added to any of this remote access software?

……

……

……

……

21. Are innovations relevant in your industry?

(a) Yes [ ] (b) No [ ]

22. Are you ready to accept and use IT innovations in your line of duties? (a) Yes [ ] (b) No [ ]

23. Are you ready to accept and use a remote system administration application that runs on a smartphone?

(a) Yes [ ] (b) No [ ]

24. If yes to question 22 above, what is your reason for accepting and using such innovation?

(a) It will eliminate restrictions to one place [ ]

(b) Administrator will be readily available always to serve [ ]

(c) It will encourage the use of portable smart devices [ ]

(d) Other specify………………………………………………………………………………………………………

Thank you for your time. If there is anything you may like to add, please write it here.

APPENDIX B

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY-KUMASI

INSTITUTE OF DISTANCE LEARNING (IDL)

QUESTIONNAIRE

Introduction

I am a student from the Computer Science Department of Kwame Nkrumah University of Science and Technology, currently undertaking a study on "A comparative study of Remote Access Technologies and proposed implementation of a smartphone app for remote system administration".

I humbly plead with you to share your sincere and candid knowledge with me through this questionnaire to provide me with good and relevant findings. Information you provide here is solely for academic purpose and would be treated with strict confidentiality. Thank you very much for your time.

Instructions:

In this questionnaire, respondents are required to tick in the appropriate box.

On a scale of 1 – 4 (i.e. 1- Excellent, 2 - Very Good, 3 – Good, 4 – Poor, 5- not available) rate the performance of this android app.

1. How do you rate the performance of the android app in terms of response time?

	1	2	3	4	5
Android app for remote system admin (secure RFB protocol)					
Remote Desktop (RDP protocol)					
VNC app (RFB protocol)					

2. How do you rate the availability of the android app?

	1	2	3	4	5
Android app for remote system admin (secure RFB protocol)					
Remote Desktop (RDP protocol)					
VNC app (RFB protocol)					