

Towards a Secure Electronic Voting System Enhanced with Mobile Telephone Technologies

Case Study: Uganda Electoral Commission

**A postgraduate dissertation
Presented to
Faculty of Science/Department of Information System
in partial fulfillment of the requirements for
the award of the degree
Master of Science in Information Systems**

Uganda Martyrs University

**Nganda Martin
2014-M132-20011**

January, 2017

DEDICATION

This piece of work is dedicated to my beloved wife Nampa Diana who has given me the reason to persist with this research. To my beloved parents who raised me up and for having always reminded me to have faith in God. To Directorate of Geological Survey and Mines for having supported me during the entire course. To my supervisor Eng. Yiga Stephen who has been guiding me throughout this research. Last but not least to the Almighty God for having given me the wisdom, courage and resources to complete this course

TABLE OF CONTENTS

DECLARATION	i
APPROVAL	ii
DEDICATION	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vii
LIST OF FIGURES	viii
LIST OF ABBREVIATIONS	ix
ABSTRACT	x
CHAPTER ONE	1
INTRODUCTION	1
1.0 Introduction	1
1.1 Background of the study	6
1.2 Statement of the problem	9
1.3 Research Objective	10
1.3.1 Main Objective	10
1.3.2 Specific Objectives	10
1.4 Scope of the study	10
1.4.1 Geographical Scope	10
1.4.2 System Scope	11
1.5 Significance of the study	11
1.6 Conclusion	12
CHAPTER TWO	13
LITERATURE REVIEW	13
2.0 Introduction	13
2.1 Benefits and challenges of Electronic Voting	14
2.2 Existing Systems	15
2.2.1 Cryptographic methods	17
2.2.2 Cryptographic Schemes	18
2.3 Mobile technology trends in 2016	22
2.3.1 The prominence of Swift	23
2.3.2 Apps fueled by cloud	23
2.3.3 New cross platform tools in abundance	23
2.3.4 Mobile pay will drive more mobile commerce	23
2.3.5 A bigger role for Beacons	24
2.3.6 Form-factors around wearables set to change	24
2.4 Hybrid Mobile Application Development	25
2.4.1 Ionic Framework	25
2.4.2 Mobile Angular UI Framework	26
2.4.3 Sencha Touch Framework	26
2.4.4 Kendo UI Framework	26
2.4.5 Conclusion	26
2.5 Implementation of a hybrid mobile application (HMA)	27
2.5.1 Architecture for implementing HMA	27
2.5.2 Tools for implementing HMA	28
2.6 Software Development Life Cycle (SDLC)	29

2.6.1	Waterfall Life Cycle Model	29
2.6.2	Spiral Life Cycle Model.....	30
2.6.3	V-Shaped Life Cycle Model	31
2.6.4	Agile Life Cycle Model	31
2.6.5	Prototyping Life Cycle Model	32
2.7	Conceptual Framework	34
2.7.1	User centered Design	34
2.8	Conclusion.....	36
CHAPTER THREE	38
METHODOLOGY	38
3.0	Introduction	38
3.1	Research design.....	38
3.2	Target Population	39
3.3	Sampling Procedures.....	39
3.3.1	Sampling technique.....	39
3.3.2	Reasons for using this sampling technique.....	40
3.4	Systems Requirements Gathering and Analysis.....	40
3.4.1	Document analysis	40
3.4.2	Paper prototyping.....	41
3.4.3	Semi-Structured Interview	43
3.4.4	Analysis of findings	43
3.5	System Design.....	44
3.6	System Implementation and Testing	45
3.6.1	System Implementation	45
3.7	Deployment	46
3.8	Ethical considerations	46
CHAPTER FOUR	47
SYSTEM DESIGN AND IMPLEMENTATION	47
4.0	Analysis of Data Collection Results	47
4.0.1	Results from Data Analysis.	48
4.1	System Requirements	65
4.1.1	Functional requirements.....	65
4.1.2	Non Functional Requirements	66
4.1.3	Software Requirements	66
4.2	System Design.....	67
4.2.1	Context Diagram.....	72
4.2.2	Dataflow diagram.....	72
4.3	Database Design.....	74
4.3.1	Conceptual and Logical Design	74
4.3.2	Physical Database Design	75
4.4	Design of User Interfaces	83
CHAPTER FIVE	84
SYSTEM IMPLEMENTATION AND DISCUSSION OF RESULTS	84
5.0	Introduction	84
5.1	System Implementation.....	84
5.1.1	System security implementation	84
5.1.2	Database Implementation.....	85
5.1.3	Business logic and User Interfaces	86

5.2	System Testing	91
5.3	Discussion of Results	93
CHAPTER SIX.....		94
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS.....		94
6.0	Summary	94
6.1	Challenges	95
6.2	Conclusion.....	95
6.3	Recommendations	96
REFERENCES		97
APPENDICES		101
Appendix 1A.....		101
Appendix 1B.....		105
Information Security Assessment Oral Interview.....		105
Appendix 2A.....		108
Appendix 2B.....		109
Appendix 2C.....		110

LIST OF TABLES

Table 3.1: A Summary of the Distribution of the Sample Size	40
Table 4.0 showing participants from Electoral Commission.....	47
Table 4.1: IT staff perspective on the importance of Information Security.....	48
Table 4.2: In-Charge of Information security at the Electoral Commission.....	49
Table 4.3: Information Security Policy awareness and use of computing facilities	49
Table 4.5: Training on Information Security and Data Protection at the EC	50
Table 4.7: Information types used by IT staff.....	51
Table 4.8: What constitutes acceptable use of Commission computers	51
Table 4.9: Do EC computers affect other staff	52
Table 4.10: Password strength according to the Commission Information Security Policy	53
Table 4.11: Security of computers during break time at EC.....	54
Table 4.12: Likelihood of opening attachments / links that are not work related	55
Table 4.13: Share of Login Credentials	56
Table 4.14: Sharing of passwords with colleagues.....	56
Table 4.15: Storage of files on the Commission computers	57
Table 4.16: Appropriate method for sending confidential information to another office	58
Table 4.17: Procedures for handling documents containing sensitive personal information	58
Table 4.18: Use of home computers to manipulate commission information	59
Table 4.19: Access to commission shared drives, files, applications or emails	59
Table 4.20: Role of IT staff in protecting Office computers and information on them.....	60
Table 4.21: IT staff interest in Office Computers.....	61
Table 4.22: Position held by the IT staff at the Commission.....	61
Table 4.23: IT staff titles that describe their roles played at the commission	62
Table 4.24: Working experience of the IT staff at the commission.....	63
Table 4.25: IT staff department or section at the commission.....	63
Table 4.26: Internet Accessibility at home	64
Table 4.27: Use of Social Networking sites by IT staff.....	65
Table 4.28: Functional requirement obtained during analysis of collected data.	66
Table 5.1: Tests Results	91
Table 5.2 Gives a Summary of the Tools Used in Implementation and Testing	93

LIST OF FIGURES

Figure 2.1: Password-based encryption	21
Figure 2.2: Framework for User centered Design	34
Figure 2.3: Shows the generic User Centered Design process	36
Figure 3.1: Prototyping Methodology.....	39
Figure 4.1: General system architecture for the eVote system	67
Figure 4.2: Technologies Architecture	69
Figure 4.3: Diagram showing the Android Architecture	70
Figure 4.4: showing the context diagram.....	72
Figure 4. 5: Data flow diagrams (DFD) showing Secure Electronic Voting System	73
Figure 4.6: EERD for Electronic evoting System.....	74
Figure 5.1: Screen shot of the eVote database with its tables in phpMyAdmi	86
Figure 5.2: Show login interface into the eVote system.....	88
Figure 5.3: Showing how to add in a new candidate details.....	88
Figure 5.4: Showing how to add in a new voter	88
Figure 5.5: Showing how to capture the fingerprint of the voter using mRegister app.....	88
Figure 5.6: Shows the mobile interface and loading of mVote app.....	89
Figure 5.7: Showing verification process of voter fingerprints to access the eVote app.....	89
Figure 5.8: Shows casting of votes by the voter	89
Figure 5.9: Shows submission of votes to EC servers.	90
Figure 5.10: Election results from EC.	90

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
ATM	Automatic Teller Machine
BVVS	Biometric Voters' Verification System
CA	Certificate Authority
DoS	Denial of Service
EC	Electoral Commission
EVS	Electronic Voting System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
IEBC	Independent Electoral and Boundaries Commission
IEC	Independent Electoral Commission
MD5	Message Digest
NIST	National Institute of Standards and Technology
PBE	Password Based Encryption
PCI DSS	Payment Card Industry Data Security Standard
PDA	Portable Digital Assistant
PKC	Public Key Cryptography
RSA	Rivest-Shamir-Adleman
SDLC	Software Development Life Cycle
SKC	Secret Key Cryptography
SOC	Service Organization Control
TLS	Transport Layer Security

ABSTRACT

With the rapid growth of the Internet and mobile technologies, electronic voting appears to be an alternative to conventional elections. Various Information Security such as cryptography, biometric authentication, are being combined with mobile telephone Technologies, which have contributed towards a secure electronic voting system enhanced with mobile telephone technologies as articulated in the literature.

Literature reviewed by the researcher indicated that a lot of work has been done by researchers around the world in the area of electronic voting. However, many electronic voting systems have failed to satisfy voters' expectations. Security is considered a big concern for electronic voting, hence drawing the attention of research over the recent years. In Uganda, the development of appropriate and scalable voting systems has been difficult to achieve. Traditional paper-based voting system currently used is associated with problems of voter lists manipulation, ballots stuffing, voter intimidation, and vote buying. Biometric voters verification systems (BVVS) used by Electoral Commission (EC) in the recent elections for voter's verification were standalone systems and not connected to EC central database servers.

In this project, the researcher developed a secure electronic voting system enhanced with mobile telephone technologies, which is suitable for voting over a biometric mobile device that is linked to the BVVS to EC database servers. The electronic voting system uses a biometric authentication method that ensures the authenticity and verification of a voter using fingerprint recognition technologies is done over mobile device. User passwords to access the electronic voting system are also encrypted using Java custom 8-steps encryption algorithms. During the voter's registration, the system captures the voter's details including the voters fingerprint patterns and the information is stored into the database. User passwords are encrypted by generating a reservation code of 6 alpha numeric characters that is random and unique safe.

During the voting process, the system verifies the voter's fingerprint patterns by matching the already existing patterns stored in the database before the voter is granted access to cast the vote. Thus, the adoption of this method eliminates the traditional use of a voters ID and ballot papers to cast the vote.

CHAPTER ONE

INTRODUCTION

This chapter focuses on the background of the study, statement of the problem, main objective and the specific objectives of the study, scope, significance of the study, and the conceptual framework.

1.0 Introduction

The project is embedded in the academic domain of security in Information Systems (IS). According to Garrity (2013), information system refers to the set of interrelated components working together to collect, process, store and disseminate information to support quick decision making, coordination, control, analysis and visualization of organizational goals and objectives. For Zwass (2016), explains information system, as an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. Information systems are used to run interorganizational supply chains and electronic markets. For instance, corporations use information systems to process financial accounts, to manage their human resources, and to reach their potential customers with online promotions. Many major companies are built entirely around information systems. These include eBay, a largely auction marketplace; Amazon, an expanding electronic mall and provider of cloud computing services; Alibaba, a business-to-business e-marketplace; and Google, a search engine company that derives most of its revenue from keyword advertising on Internet searches. Governments deploy information systems to provide services cost-effectively to citizens. Digital goods such as electronic books, video products, and software and online services, such as gaming and social networking, are delivered with information systems. Individuals rely on information systems, generally Internet-based, for conducting much of their personal lives: for socializing, study, shopping, banking, and entertainment.

Kissel (2013), argues information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The sub domain of the project is information security. Mulalira (2016) defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, recording or destruction of data. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form (i.e., electronic (cyber) or print (hardcopy)). Rouse (2016), also defines information security (infosec) as the set of business processes that protects information assets regardless of how the information is formatted or whether it is being processed, is in transit or is being stored. Information security is not a single technology; rather a strategy comprised of the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Processes and policies typically involve both physical and digital security measures to protect data from unauthorized access, use, replication or destruction.

According to Kissel (2013), describes information systems security as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

From the above information, organizations nowadays rely mainly on information to make decisions, carry out their activities and meet regulatory requirements. As a result, information is now considered an important resource to be protected. Ensuring the confidentiality, integrity and availability (CIA) of an organization's information has become a difficult task, which should be carried out on an ongoing basis. Information security standards provide organizations with the tools to help them define an information systems security strategy scaled to their business needs and contractual or legislative requirements. These numerous information security standards include;-

- a) ISO 27001;
- b) ISO 27002;
- c) SOC 1 - SSAE 16, SOC 2 and SOC 3;

- d) PCI DSS;
- e) National Institute of Standards and Technology (NIST) standards

Looking at the trends of the information security around the world, Swart (2015), argues that while policies around cyber security are good to have, however the policies alone lack the potential to quantify data, and countries need to establish what their ICT assets are and what vulnerabilities are within them.

In Africa, according to Kileo (2015), cybercrime statistics show Africa is at risk as internet use increases. Basie (2015), adds on that South Africa lacks a cyber security culture, as the country is yet to implement some of the critical policies adopted by the African Union Convention on Cyber Security and Data Protection. Although Tanzania has big investments in fibre-optics which are over 70% coverage of fibre, and has been described as low-risk, it is bordered by high-risk countries such as Kenya and Congo. In 2012, around 999 cybercrime cases in Tanzania were realized, very hard to prosecute as there was no legal framework to deal with crimes of this nature. ATM fraud is vast, costing the country a great deal of money, and the country also experiences the theft of information, stalking, piracy, identity theft, drugs and human trafficking (Kileo, 2015).

In Uganda, Mulalira (2016), explains cybercrime as a criminal activity done using the computer over the internet to perform illegal acts such as cyber terrorism, intellectual property infringement, internet usage policy abuses, internet fraud, industrial espionage and altering of data, piracy, impersonation and hacking, remain a challenge. Twesigye (2013), argues that increased record of electronic based frauds during 2011, 2012 and 2013 were highly realized which included ATM and electronic payment card skimming, email hacking, password theft using key loggers and social engineering tactics, phishing, botnets and mobile money frauds. The threat is no longer limited to only IT staff since social engineering and dumpster diving are leading factors for fraud.

In conclusion, there is no information system with ultimate information security due to the massive cybersecurity faced by the world around although with use of mobile technologies, has led to development of information systems and mobile applications with better security features.

According to Daichendt (2015), mobile technology refers to any device that you can carry with you to perform a wide variety of tasks. It is technology that allows those tasks to be performed via cellular phone, PDA, vehicles, laptops, etc. A standard mobile device has evolved from a simple two-way pager to being a cellular phone, a GPS navigation system, a web browser, and instant messenger system, a video gaming system, and much more. This includes the use of a variety of transmission media such as: radio wave, microwave, infra-red, GPS and Bluetooth to allow for the transfer of data via voice, text, video, 2-dimensional barcodes and more. Swaddle (2016) argues that mobile is everywhere consumers are. In fact, there are now more mobile devices in the world than people. People around the world use mobile devices to research, vote electronically, shop, compare products and services, read and write reviews, anytime and everywhere. In today's always-on world, a great mobile customer experience is critical. Added to this is the fact that mobile apps are now an inseparable part of our daily lives and purchases made through mobile devices are set to double in the year ahead.

Okediran et.al, (2011) defines electronic voting as a term which refers to various voting processes where computers or digital devices are used to cast and count votes. The process can also involve transmission of ballots and votes via public networks. Therefore, an electronic voting framework is a voting framework in which the election data is recorded, stored and processed primarily as digital information. An election is the formal process of selecting a person for public office or of accepting or rejecting a political proposition by voting (Britanica, 2015). Free and fair elections are a fundamental aspect of modern democratic governance. In order for candidates and voters to have faith in the election process, it is essential that election systems are transparent and resistant to manipulation. Elections and voting are fundamental to any consensus-based society (Okediran et.al, 2011). A well-designed election system must provide several features including Accuracy: An election system must accurately reflect the intent of each individual voter.

The system must be secure against parties attempting to manipulate the outcome of voting system, including ballot stuffing by voters or intentional miscounting of votes by election officials. Anonymity: A voter's identity must not be able to be connected with their vote, in order to prevent voters being subject to reprisal for voting against a particular candidate.

Accessibility: the system should allow for all voters to cast their ballot, regardless of age or disability. For e-voting system to be secure, the system has to provide security properties as follow;-

- a) Privacy, The identity of a voter cannot be linked to her vote. This is a key aspect for any election because it allows the voters to freely decide the option they prefer without making it public. There are some related properties like vote selling prevention or coercion resistance that are also desirable. In the first one, voters are not able to prove how they voted, despite being able to provide evidence that they have cast a vote. The fact that there is an evidence of their votes would make them easier to be coerced. Some coercion-resistance techniques provide tools that allow voters to cheat the coercers. Coercers are tricked into thinking that the voter has behaved under coercion.
- b) Integrity, The result of the election cannot be altered in any way. Each voter should be confident about her vote being properly tallied. This means that all the votes have been casted as they were intended to be, and after that, the votes have not been altered during their processing. Integrity also ensures that only voters in the electoral roll are able to cast a vote, and that no more than one vote from each voter will be tallied.
- c) Robustness, This property refers to the strength of the system against attacks. The system should be able to face situations in which some voters are misbehaving so as to disrupt the process.
- d) Verifiability, The verifiability provided by traditional elections involves trusting in audit parties. By contrast, electronic elections allow the voters to verify the integrity of the voting process.

1.1 Background of the Study

As democracies across the globe fight challenges related to electronic voting systems, here a secure e-voting system enhanced with mobile telephone technologies, gives a promising research. Okediran et.al, (2011) defines E-voting as a term which refers to various voting processes where computers or digital devices are used to cast and count votes. It can also involve transmission of votes through public networks. Therefore, an electronic voting framework is a voting framework in which the election data is recorded, stored and processed primarily as digital information. New technologies have a vast potential for empowerment which needs to be fully exploited.

Mourine and Ephias (2013), stated that e-voting and counting technologies are increasingly being used around the world with India and Brazil taking the center stage. Among other countries that have adopted electronic voting and counting technologies for their national elections are Belgium, Philippines, Estonia, Norway, Pakistan, United States and United Kingdom. These countries are at various stages of piloting and using e- voting systems and introduction of Internet voting.

In Africa, a good reference is South Africa which held its first democratic election in 1994 conducted by the Independent Electoral Commission (IEC) of South Africa with international observers in attendance, both bodies declared the electoral process “free and fair” (Mourine and Ephias, 2013). According to Mourine and Ephias (2013), the IEC has been responsible for the implementation of the electoral system for elections in South Africa since the first democratic elections. The method used for this process where both manual ballot papers and e -voting. After the electoral exercise, the IEC provided the possible drawbacks to the current electoral systems according to the South Africa information. The first being the number of illiterate adults in South Africa, other contributing drawback to the current electoral system are the level of poverty in South Africa, voters complain of the long distance they have to travel in order for them to reach polling stations which has often resulted into a decline in voter participation. In addition, there is difficulty in accessing some parts of the country and cost of the physical ballot materials of the paper based electoral system.

According to a survey done by Citizen Surveys in October and November 2008, concern in voter confidence of the ballot forms were revealed (Citizen Surveys, 2008). It is clear that the current paper-based electoral process used in South Africa can be significantly improved to mitigate some of the challenges it is faced with. Electronic voting however is suggested as an important step towards mitigating this effect.

In East Africa, the Independent Electoral and Boundaries Commission (IEBC) of Kenya attempted to use an electronic voting system during the March 2013 elections, this was a direct response to the challenges Kenya faced in the 2007 and 2010 elections (IEBC report, 2013). The system was implemented using a combination of biometric voter registration which was to capture fingerprints, photos and textual information about every voter and electronic poll books, which were able to validate every voter's fingerprint before access to ballot is given. The electronic poll book was also developed to allow the IEBC know, in real time how many voters came to a polling station to cast their ballots at any point during the day and results tabulation. The computer system was able to check the number of votes reported on the tally form with the number of actual voters who came to the polling station and automatically reject any report where the number of votes is higher than the number of voters in a polling station. The e-voting trial was not very successful as shown by various reports (IEBC report, 2013). Kenyan voters were frustrated with delayed results after electronic system fails. This e-voter system made the Kenyan elections to struggle, with failure of electricity, crushing software, an overloaded SMS network for reporting results and a glitch that may have disqualified more than a quarter-million votes. The errors led the losing candidate to claims that the election was rigged.

According to Deutsche Institut für Entwicklungspolitik Report (2011), insecurity still seems to be commonly associated with voting in Sub-Saharan Africa (SSA), with eight of the 20 countries witnessing downward security trends in the context of recent elections. Most of these countries have experienced armed conflict in the last 10 years (Awad and Ernst, 2011). Naturally, the cases with major downward security trends at election time were also those where contention was high. Uganda being one of the countries in SSA hasn't survived this as well.

Elections in Uganda have however mostly been held over the past years using the manual paper ballot method, it has been very difficult to embrace the idea of e-voting method because the systems for self-identification such as unique personal National Identity card numbers, or any other personal User IDs for purposes of the personal unique identification are not in place.

Chipfunde (2016) stated that the use of the Biometric Voters' Verification System (BVVS) was seen to be a good practice for fraud prevention and identity verification mechanism during the 2016 General Election in Uganda. The aim of the system was to strengthen the identification of voters through biometrics so that no one votes more than once in a particular election, however the system was abandoned at few centres due to human errors like putting wrong access codes, software failures and lack of operational skills thus making BVR not a silver bullet in solving all electoral issues in Uganda. The Electoral commission was forced to use back the traditional voting system associated with problems of voter lists manipulation, ballots stuffing, voter intimidation, and vote buying. Chipfunde (2016) explains that the traditional system involved hard copies of the voter lists with photographs which the presiding officers would use to identify voters and these lists were available at each polling station as an alternative option in case of technology failure.

According to Sekaggya et.al, (2010), traditional paper ballot system of voting under Electoral Commission is still existing in the country. Voter registration and polling processes, which fall under the EC's mandated activities, have been continually flawed and heavily criticized. Problems with the voters' register cited in previous elections, including duplicate names, missing names, and names registered in the wrong district, have not been adequately addressed, and have already been seen in advance of February 2016.

The traditional paper-based voting system currently used is being severely judged after having found evidences of misbehaving parties. The confidence on the fairness of an election is getting lower as some information about suspicious results gets filtered. The system is associated with problems that include voter lists manipulation, ballots stuffing, voter intimidation, and vote buying. There is controversy over the way that votes are counted, tallied and transmitted.

Although the EC established a National Tally Centre, accessible to representatives from all political parties, to receive and verify results from the District Tally Centres, many critics feel that the use of telephones to convey results from districts is neither secure nor reliable (Sekaggya et.al, 2010).

1.2 Statement of the Problem

Over recent years, researchers have made significant efforts to design and implement electronic voting systems specifically to developing countries. While e-voting has been an active area of research for the past two decades, efforts to develop real-world solutions have just begun.

In Uganda, the development of appropriate and scalable voting systems has been difficult to achieve. The literature reveals many voting systems that have not survived the test of time (Feras, Mutaz and Khairall, 2011).

In Uganda today, traditional paper-based voting system currently used is associated with problems of voter lists manipulation, ballots stuffing, voter intimidation, and vote buying.

The voting centers are often heavily staffed to administer identity check, voting eligibility, and ballot dispersal. Some staff members unfaithfully enforce the regulations for the benefit of their favorite candidates. The biometric voters verification systems (BVVS) used for voter's verification are not linked to EC central database servers. They are standalone systems. A copy of the database is uploaded to the BVVS through use of the memory cards. These problems have lowered trust in the political system and electoral processes and, consequently, adversely affecting participation in the political life as observed in the recent general elections, February 2016. Therefore, as the computing, communicating, and cryptographic techniques progress rapidly, increasing emphasis has been placed on developing voting schemes that uses information and communications technology resources for providing more efficient voting services than conventional paper-based voting methods. Therefore there is a need for a better, faster, more convenient and secure electronic voting system enhanced with mobile phone technologies to prevent opportunities for fraud and sacrificing the voter's privacy, authenticity and integrity.

1.3 Research Objective

The Research Objectives of the study were categorised into major and specific objectives. The major objective of the study describes the intentions of the research while specific objectives describe the steps carried out to achieve the major objective.

1.3.1 Main Objective

The main objective of this project is to implement a secure electronic voting system enhanced with mobile telephone technologies that is linked to the EC's central database, enable voting process done on the mobile devices, provides voter's privacy, integrity, with accuracy, mobility, authenticity, non-repetition mechanism and trusted electronic voting in addition to the requirement for electronic voting.

1.3.2 Specific Objectives

The specific objectives are the following;

1. To review the current system and literature related to secure information system and mobile voting system so as to understand their strengths and weaknesses
2. To design a user centered e-voting architecture so as voters cast their votes
3. To develop a system that will help the Electoral Commission to conduct their elections online so as to minimize on the cost and time spent during the entire electoral process
4. To test the system so as to ensure the system is working properly and ready for use.

1.4 Scope of the Study

This section describes the geographical and content scope within which the researcher carried out the study.

1.4.1 Geographical Scope

The system will be developed for Electoral commission. Electoral commission is a government body in Uganda whose mission is to organize and conduct regular free and fair elections and referenda professionally, impartially, and efficiently.

The system is designed to cater for only two divisions in the central and will be managed by the Chairperson with the electoral team at Electoral commission.

1.4.2 System Scope

The system developed is able to register voters, candidate for electoral posts and administrators in case more than one administrator is required. The system is also able to meet the requirements that are needed of the e-voting system. These requirements are as follows;-

- a) Privacy: Voters remain anonymous, Authenticity: Only eligible voters can cast their votes;
- b) Integrity/accuracy: Once a voter cast a vote, no alternation to this vote is permitted;
- c) Security: Throughout the voting process, a vote can't be tampered with;
- d) Democracy: All eligible voters must be able to vote, one person-one vote and no one can vote more than once or vote for others;
- e) Multi-user: A number of voters can vote simultaneously;
- f) Accessibility: The system can be accessed by voters from any location using secure Internet and mobile devices; and
- g) Availability: The system must have high-availability during the electoral process.

1.5 Significance of the Study

Electronic voting systems potentially reduce or remove unwanted human errors. In addition to its reliability, electronic voting can handle multiple modalities, and provide better scalability for large elections (Norbert, Ronald and Jürgen, 2008). E-Voting is also an excellent mechanism that does not require geographical proximity of the voters (Adem and Metin, 2011). For example, voters abroad can participate in elections by voting online. The study therefore relieves both the EC and the voters of the tedious experience that comes along with voting. EC also takes benefit of e-voting by having a reduced cost of running the elections. Hence improved voter participation and the implemented measures that protect their privacy and rights. Furthermore, the developed system seeks to provide literature for future researchers in form of literature.

1.6 Conclusion

The project, focused on the development of a secure electronic voting system with mobile telephone technologies that can be adopted for any electoral body in developing countries in this case Electoral commission. The developed solution was motivated with managing the weaknesses associated with any voting system; this was achieved by the implementation of a secure web based electronic voting system that was able to provide a secure workflow of the entire electoral process.

A background to the aforementioned problem was discussed at length and consequently a clear description or statement of the problems associated with e-voting was defined. The project's objectives were clarified to that effect, along with a scope that stated what is to be included in, or excluded from the system. This means a clear definition of time, geographic, deliverables, data, and functionality of the secure web based electronic voting system.

In addition to the above, the significance, contributions or importance of the system to the relevant stakeholders most notably efficiency and accurate delivery of results were identified. This project also seeks to experiment the use of a participatory approach in systems design. In this case the system users are involved in the systems design. Implementation of a secure web based electronic voting system is a promising, applicable and effective tool for voting that will make easy the entire electoral process.

CHAPTER TWO

LITERATURE REVIEW

This chapter is based on reviewing the literature that is relevant to the research project. The literature was obtained from different scholars that have published works related to the main and specific objectives of the research. Below is the discussion focused on electronic voting systems with mobile telephone technologies, their benefits and challenges during voting processing and research methodologies reviewed.

2.0 Introduction

Literature suggests that improvements in voting systems started as early as in 1892 with the introduction of the lever arch machine, then the introduction of optical-scan machines and punch card systems for voting (Ofori and Paatey, 2011, p. 92). The next evolution saw the introduction of Direct Recording Electronic (DREs), Telephone, Kiosk, Internet voting systems and lastly the mobile phone voting systems (Okediran et al., 2011, pp. 135-142). Electronic voting (e-voting) has been attracting a lot of attention and research for the past few years all over the world, for it has some remarkable advantages over traditional paper-based voting. According to Mohammad and Morshed (2013), Electronic voting is already in use in many countries around the world. It is proved that electronic voting speeds up the counting of votes and improves turnout among disabled voters. E-voting systems have the potential to improve traditional paper-based voting procedures by providing convenience and flexibility to the voter (Okediran et al., 2011, p. 13).

Literature to be reviewed for electronic voting was chosen basing on existing research from major scholarly books and journal articles in the relevant area of voting which in many subjects gave more up-to date material. The review was also based methodological review where reviewing methods of analysis provided a framework of understanding at different levels [those of theory, substantive fields, research approaches, and data collection and analysis techniques].

It also focused on how researchers drew upon a wide variety of knowledge ranging from the conceptual level to practical documents for use in fieldwork in the areas of ontological and epistemological consideration, quantitative and qualitative integration, sampling, interviewing, data collection, and data analysis. This approach helped to highlight ethical issues which the researcher should be aware of during literature review.

2.1 Benefits and challenges of Electronic Voting

An electronic voting is an electronic system which uses election that would allow voters to transmit their secure and secret voted ballot to election officials over the internet. Ananda, (2016) suggests that electronic voting is convenient because with the well-designed software and system, the voters can simply use their own equipment with the minimal time and skill to finish the voting process; With Mobility, voters use mobile devices such as iPad, Samsung galaxy and, iPhone to vote any time anywhere; Using electronic voting saves money from reducing the personnel expense for example, expense for location management and administration fee; Go green saving the paper by using online voting; Tally process is speedy. By clicking just a small button can submit your voting to the system, and process is much faster than the traditional ballot counting method operated by people.

Despite the particular advantages to electronic voting system, Ananda, (2016 p.27) argues about the security issue and the unequal access chance to the internet are the main drawbacks to the system. Furthermore, inequality problem because for those people with low salary might not able to afford the equipment for electronic voting. They are not able to use the computer facility might lose their privilege in voting. Secondly, the system is vulnerable to security. Attacks that may occur at the client end are brute force attacks, dictionary, denial of service attacks (DoS) and viruses on the user browser. The transmission may also be attacked by interception of the communication lines, such attacks are man in the middle, eavesdroppers and network sniffers. At the server end however, a database attack may occur. Client end attacks are quite common.

2.2 Existing Systems

According to Yi, Cerone and Zhang (2006) propose mobile phone voting system developed on modular square root and blind signature system. System uses confidentiality of voter, secrecy of ballot, voter anonymity and no computation cost and communication overhead.

CA (certificate authority) involve as third party that is to say, distribution of certificates to voters is the responsibility of CA for authentication purposes, delayed occurred which make the process slow.

From the above system, there is a challenge of time delays experienced during the voting process. This is mainly because the voters have to go through authentication third party for voter's verification. More work is also required to deal with the trust retained on authentication server, end-user device (ME) and application security to improve on the voter's verification process.

Qiu and Zhu (2010), proposed GSM based mobile phone voting system which is used to cast vote without registering for voting in advance and going to polling booths. System also provide voter's privacy, integrity, accuracy, mobility, authenticity and non-repetition mechanisms.

However in above system, information stored in the database is not highly encrypted to be free from system attacks. Thus, the system lacks highly secured encryption technique for the server and database security.

According to Shaun and Choudhry (2011), proposed a mobile phone voting system based on public key encryption algorithm RSA. Proposed system contain three parts: access control; voting and election administrator server. First part holds validation and identification for the voters. Voting part done by ciphering voter data using RSA algorithm And last part is the election administrator server classifies ending result using decryption RSA private key for received encrypted data.

However the above system does not provide users with online registration which would enable users to register from anywhere as long as there is a connection to the system. Furthermore, it experiences more expensive computational cost and communication overhead due to RSA algorithm.

According to IEBC report (2013), Kenya attempted to use an electronic voting system during the March 2013 elections, this was a direct response to the challenges Kenya faced in the 2007 and 2010 elections (IEBC report, 2013). The system was implemented using a combination of biometric voter registration which was to capture fingerprints, photos and textual information about every voter and electronic poll books, validate every voter's fingerprint before access to ballot is given. The electronic poll book was also developed to allow the IEBC know, in real time how many voters came to a polling station to cast their ballots at any point during the day and results tabulation. The computer system was able to check the number of votes reported on the tally form with the number of actual voters who came to the polling station and automatically reject any report where the number of votes is higher than the number of voters in a polling station.

However in the above e-voting system, Kenyan voters were frustrated with delayed results after electronic system failure. This e-voter system made the Kenyan elections to scramble with failure of electricity, crashing software, an overloaded SMS network for reporting results and a glitch that may have disqualified more than a quarter-million votes. The errors led the losing candidate to claims that the election was rigged.

Kogeda and Mpekoa (2015) proposed a mobile phone voting system that allows the voters to instantly cast a vote without the limit of time and place, reduce fraud and increase efficiency and lower costs of running elections. Also proposed a prototype application to be installed on user mobile phones which is simple, with limited pictures or graphics for inexpensive mobile devices.

However in the above system, there is a constraint of installing prototype application on every voter's mobile phone due to different mobile platforms. The prototype application is not compatible all the mobile platforms, only compatible with android mobile phones excluding IOS phones.

In summary, this literature shows that the majority of the e-voting systems have been enhanced with mobile technologies but security and audit trail are still major challenges faced by mobile phone voting system.

The proposed system will therefore focus on making electronic voting system more secure by encrypting information in the database using Java custom 8- step algorithms. There will be no need to be in a queue while waiting to cast the vote, voting at any time of the day/night will be possible. The proposed system also provide voter verification by biometric mobile device and voting mechanism on the same mobile device. After the registration of voter's details in the system, verification and casting of vote's process will follow and then results displayed at EC's dashboard instantly for decision making.

2.2.1 Cryptography Methods

According to Kessler (2010), cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is categorized below basing on the number of keys that are employed for encryption and decryption, and further defined by their application and use.

- a) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- b) Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- c) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

In summary, public –key cryptography is proposed in the design of the new system to address the security mechanisms of confidentiality, integrity and availability of the electronic voting system and also to protect the identity of the voters.

2.2.2 Cryptographic Schemes

Two cryptographic schemes employed in E-Voting are Diffie-Hellman key exchange and password-based encryption (PBE).

a) Diffie-Hellman Key Exchange

The key exchange enables two users to exchange a key securely that can then be used for subsequent encryption of messages. It provides a method to create a shared secret key by exchanging public keys. Two users, who want to communicate, must have global public elements: prime number p and base g . User A generates key X_A , by selecting a number less than p . Its public key, Y_A , is calculated using a formula: $g^{X_A} \text{ mod } p$. User B also does the same thing producing its private key X_B and public key Y_B . Each side sends their public keys to each other. Then each side does the key agreement process. For User A, it generates the secret key, K using the formula $(Y_B)^{X_A} \text{ mod } p$. For user B, the same secret, K is generated by $(Y_A)^{X_B}$. The RSA private key is too long for people to remember. Therefore it is normally stored in a medium like diskette or smart card. To preserve its confidentiality, the key need to be encrypted. E-Voting encrypts the private key with a user password. The password is hashed using a message digest algorithm, SHA-1 and the resulting digest is used to construct a binary key for Twofish-CBC. A salt, random number, is added to the algorithm to make the key difficult to break [7]. The private key, salt and user password are passed to the PBE cipher to produce a cipher text, C . The salt and the cipher text are combined together, $\{ \text{salt}, C \}$. Mod p . When user wants to retrieve the private key, user must provide the password. The cipher text, C , the salt and the password are passed to the cipher to produce back the private key.

However Diffie-Hellman Key Exchange has weaknesses of; the Logjam (and Another) Vulnerability against Diffie-Hellman Key Exchange, According to Schneier (2015), Logjam is a new attack against the Diffie-Hellman key-exchange protocol used in TLS.

The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection. The attack is reminiscent of the FREAK attack, but is due to a flaw in the TLS protocol rather than an implementation vulnerability, and attacks a Diffie-Hellman key exchange rather than an RSA key exchange. Servers supporting DHE_EXPORT ciphers are affected by the hacker including all modern web browsers. 8.4% of the top 1 Million domains were initially vulnerable.

According to Adrian D et al (2015), Diffie-Hellman key exchange is a cornerstone of applied cryptography, but we find that, as used in practice, it is often less secure than widely believed. The problems stem from the fact that the number field sieve for discrete log allows an attacker to perform a single precomputation that depends only on the group, after which computing individual logs in that group has a far lower cost. Although this fact is well known to cryptographers, it apparently has not been widely understood by system builders. Likewise, many cryptographers did not appreciate that the security of a large fraction of Internet communication depends on Diffie-Hellman key exchanges that use a few small, widely shared groups.

In conclusion, cryptographers and creators of practical systems need to work together more effectively. System builders should take responsibility for being aware of applicable cryptanalytic attacks. Cryptographers should involve themselves in how crypto is actually being applied, such as through engagement with standards efforts and software review. Bridging the perilous gap that separates these communities will be essential for keeping future systems secure. Despite of the weaknesses faced by the Diffie-Hellman key exchange, encryption-decryption algorithms are borrowed from this scheme to design the proposed system while keeping in mind that there is a need for software reviews as technology changes to avoid system downgrades.

b) Password-Based Encryption (PBE)

According to Mohan (2015), users encrypt and decrypt their files with an easy to remember password (key) and at the same time be confident that their files are secure from prowling eyes. Public key encryption requires the secure storage of the private key.

The loss or compromise of the private key can be disastrous to the user. Password based encryption (PBE) was designed to solve problems of the kind described above. A PBE algorithm generates a secret key based on a password, which will be provided by the end user. Currently there are two standards (PKCS #5 and #12) that define how a password can be used to generate a public key code.

Mohan (2015) argues that a good PBE algorithm will also mix in a random number called the salt along with the password to create the key. Without a salt, the hacker can perform a brute force search for the key-space with relative ease. PBE is typically used in systems such as local file encryption tools, which are used to ensure data confidentiality. They are also used as a mechanism to protect the user's private key store (such as the PKCS #8 based protection of private keys). User prompted passwords are typically either a subset of ASCII or UTF-8 for purposes on inter-operability. It should be noted that UTF-8 is a superset of ASCII. The salt is a value that can thwart dictionary attacks or pre-computation attacks. An attacker can easily pre-compute the digests of thousands of possible passwords and create a “dictionary” of likely keys. Recall the fact that when you perform the digest, changing input data even a little changes the resulting digest. By digesting the password with a salt, the attacker’s dictionary is rendered useless. The attacker will need to search through passwords for each value of the salt. Alternatively, the attacker has to wait until a password operation is performed and the salt used in that particular operation is captured. Because the salt is random in nature, it is highly unlikely that the same salt will be used for the next encryption process thus limiting the attacker further. The salt needs to be generated using a pseudo random number generator (PRNG). It is also strongly recommended not to reuse the same salt value for multiple instances of encryption. Note that the salt is not a secret value. So, it can be transmitted along with the cipher-text to the receiver or via out-of-band transmission methods. Ideally the length of the salt should be same as the output of the hash function being used.

Mohan (2015) explains that iterations, another important deterrent that can be used to thwart the advances of the attacker is to include an iteration count. This will complicate the key derivation function by performing a number of iterations. The iteration count increases the cost of exhaustive password search attacks by a significant amount.

A minimum of 1000 iterations is recommended for minimum-security requirements. Just like the salt, the iteration count does not have to be kept a secret and can be transmitted in the clear along with the cipher-text if necessary. Usually the salt, the iteration-count value and are sent to the receiver as a part of the algorithm identifier value.

Mohan (2015) argues that the most rudimentary of the standards available for PBE is PKCS#5 v1.5. The following Figure 2.1 illustrates the process of generating a secret key using the PKCS#5 v1.5 standard. The salt is appended to the password before being digested using one-way functions such as MD5 or SHA-1. The choice of the digest limits the key size that can be derived using the standard. MD5 gives a digest of 128 bits and SHA-1 results in a 160-bit digest. In the Figure 2.1 below, if we used MD5 as the digest algorithm, the end result of this process will be 16 bytes (128-bits) of data. Since most symmetric ciphers need an Initialization Vector (IV) for their operation, only 8 bytes (64-bits) can be used as key material for the cipher. Thus, this particular standard can be used to generate 64-bit secret keys or weaker.

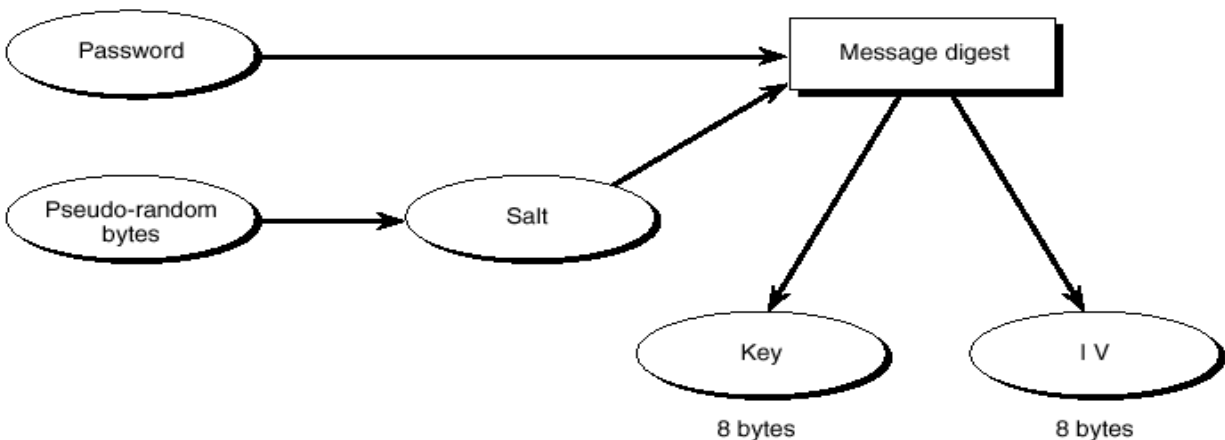


Figure 2.1: Password-based encryption as shown by Mohan (2015)

In order to generate stronger keys, we need to use standards such as PKCS#5 v2.0 or PKCS#12. The length of the keys that can be generated by these two standards is essentially unlimited. These two standards also go much beyond simple key generation and key derivation functions for password-based encryption.

They also have support for password based message authentication schemes. Incidentally PKCS#5 v2.0 supersedes the PKCS#5 v1.5 standard, but includes compatible techniques too. In general, the PKCS#5 v2.0 and PKCS#12 standard can be used in both “password secrecy” and “password integrity” modes. The password privacy mode generates a secret key for encryption and the password integrity mode generates a Message Authentication Code (MAC) key.

However Password-Based Encryption (PBE) has weaknesses of; the PBE standards leave some areas open to the discretion of the developer. For example, the choice of the password is not limited in any way by the standards. It is up to the application to determine whether the chosen password is strong or weak.

The standard also does not specify the format for the password. But, to be fully interoperable with most applications, it is suggested that developers use ASCII strings and not local strings (Mohan, 2015).

In summary comparing weaknesses of the two cryptographic schemes, Java custom 8-step encryption (Password Based Encryption) is proposed to be used for the new system because the user requires an easy-to-remember passphrase at least one that's made of recognizable characters and short enough to write down and yet for secure encryption by today's standards, at least 128 strongly random bits are required to secure the system. PBE is also used in applications where an attacker can repeatedly try to guess the password undetected and beyond the control of the genuine sender/recipient.

2.3 Mobile Technology Trends in 2016

According to Daichendt (2015), mobile technology refers to any device that you can carry with you to perform a wide variety of tasks. It is technology that allows those tasks to be performed via cellular phone, PDA, vehicles, laptops, etc. A standard mobile device has evolved from a simple two-way pager to being a cellular phone, a GPS navigation system, a web browser, and instant messenger system, a video gaming system, and much more. This includes the use of a variety of transmission media such as: radio wave, microwave, infra-red, GPS and Bluetooth to allow for the transfer of data via voice, text, video, 2-dimensional barcodes and more.

Looking the trends in mobile technologies around the world, Swaddle (2016) gives his views as following;-

2.3.1 The prominence of Swift

Swift, the latest programming language from Apple has harvested a lot of attention from tech communities and particularly from developers. The language is designed to work both as an application language and a systems language, and offers greater reliability when writing code. This is quite clearly demonstrated by the fact that since its release in September 2015, Swift has enjoyed 11 million downloads.

Swift is also faster than Objective C and is the biggest release for a rapid app development environment. The new programming language of 2016 have taken a lead in developing diverse apps for iOS, OS X, Apple Watch OS, and Apple TV OS apps.

2.3.2 Apps fueled by cloud

With mobile and wearable devices making the need to access apps and data from any device and location a necessity, cloud is naturally taking a central role for the vast majority of apps. As integration and synchronization of apps across multiple devices continues to grow, so cloud driven apps are being adopted by more businesses and developers in 2016.

2.3.3 New cross platform tools in abundance

With the simultaneous and often competitive growth of several mobile platforms, and the rise of wearable tech and smart TVs that we witnessed this year at Customer Electronic Show (CES), no business would consider developing an app for a single platform. With a vast array of devices and their advanced features and functionalities, apps need to address the requirement for multiple platforms and devices and have a cross-platform development approach such as PhoneGap, Appcelerator, Sencha, Titanium, Unity3D, Cocos2d, and many others.

2.3.4 Mobile pay will drive more mobile commerce

Several big ecommerce leaders have shut their websites and begun operating as app-only businesses, and there are many other electronic commerce companies who give more priority to mobile traffic in their decisions.

This might surprise you to know that around 90% of internet traffic is as a result of people accessing the online store from either smartphones or tablets and there is no sign of this trend narrowing in the near future. Especially with technologies like Mobile Pay being offered across platforms and devices. The integration of wallets and devices has become even stronger in 2016 and so too will the integration of ecommerce and mobile.

2.3.5 A bigger role for Beacons

GPS-based technologies like Beacons have revolutionized the business marketing, promotion and shopping experience. At the beginning of 2016, Beacons became stronger, guaranteeing location tracking benefits for several niche markets aside from retail. Brands like General Electric have already ventured into incorporating Beacons into a range of lights made for retail stores, and the technology has also prompted interest from security agencies. So, through Beacons, location tracking has continued to experience new applications for businesses and other civic purposes.

2.3.6 Form-factors around wearables set to change

After the development of google glass and apple watch two years back, now the focus is put more on making wearable form factor better so the devices are richer in experience than simply offering another smartwatch or optically mounted computer. Smartwatches are already showing signs of becoming fully standalone mobile devices and 2016 was just the beginning. Wearables are set to be more fashionable, moving away from being just gadgets that no one actually wears. New devices launched at CES seem to be moving away from the traditional watches and wristbands.

In summary, mobile is everywhere consumers are. In fact, there are now more mobile devices in the world than people. Customers are using mobile devices to research, shop, compare products and services, read and write reviews, anytime and everywhere. In today's always-on world, a great mobile customer experience is critical. Added to this is the fact that mobile apps are now an inseparable part of our daily lives and purchases made through mobile devices are set to double in the year ahead.

2.4 Hybrid Mobile Application Development

Oskar, (2013) argues that a hybrid application is basically a web application that runs in a native shell. The application is usually written in framework such as phonegap using HTML, CSS and JavaScript.

The use of the native shell allows hybrid applications access more device capabilities than the standard web application. Some of those capabilities are the accelerometer and the camera built into the devices. This kind of application is also distributed through the application markets.

2.4.1 Ionic Framework

Bala, (2015) defines ionic as a complete open-source SDK for hybrid mobile app development. Built on top of AngularJS and Apache Cordova, Ionic provides tools and services for developing hybrid mobile apps using Web technologies like CSS, HTML5, and Sass. Dario (2016) argues that Ionic is a framework on top of Cordova which is a framework for building hybrid apps.

i. Benefits of Ionic Framework in Mobile App Development

There are few benefits of Ionic framework, and some of them have been explained below:

- a) **Platform Independent Framework**, ionic has the ability to acknowledge the platform specific optimized CSS equivalent to the native look and feel on various mobile Operating Systems. It reduced the need for code rewriting as it provides the codes of mobile-optimized HTML, JS, and CSS components. Apart from this, ionic integrates into AngularJs which becomes a robust structure making code excellent as well as more manageable. This empowers the startup entrepreneurs to come out with newer concepts at reduced budget.
- b) **Default User Interface**, the framework has many default CSS and JS components that cover most of the essential/basic things which the programmer wants to create into a mobile application. Some of them include sliding menu, form inputs, buttons, navigation, tabs, sliding boxes and many more. The default styles are extremely elemental. One can undoubtedly customize them by adding pre-defined CSS classes to the element.
- c) **Feasible Cross Mobile App Development**, developing an application at once is very essential as it would be compatible with all the mobile devices.

However, it needs extremely limited use of time, assets and efforts, and helps in giving a unified look and feel. Beside, Ionic assists in building applications rapidly with expertise, and deploys standard tools with a single code base.

- d) **Built on AngularJS**, ionic is developed on top of the AngularJS framework. On a very basic level, Ionic expands AngularJS with features to make creative mobile applications. Furthermore, Ionic framework shares compatibility with AngularJS, thus, the benefits of AngularJS development can be put to use too.

2.4.2 Mobile Angular UI Framework

Raj (2014) addresses mobile angular user interface as an HTML 5 framework which uses bootstrap 3 and AngularJS to create interactive mobile apps. The main features of mobile angular user interface include;-bootstrap 3 and angularjs (angular-route, angular-touch and angular-animate) however bootstrap 3 module component are missing such as switches, overlays and sidebars.

2.4.3 Sencha Touch Framework

Sencha Touch is an HTML 5 mobile app framework for creating apps for several platforms including iOS, Android and Blackberry. Raj, (2014) argues that sencha touch isn't that difficult to use but in order to get the best out of Sencha Touch, the programmer needs to invest in a considerable amount of time.

2.4.4 Kendo UI Framework

Telerik's Kendo UI is an HTML 5 framework for creating cross platform mobile applications. Kendo UI relies heavily on jQuery and has a number of jQuery based widgets, toolset and javascript framework features. However most of the commonly used widgets are still under a commercial license (Raj, 2014).

2.4.5 Conclusion

Using the hybrid application approach allows the programmer to write apps as they were webpages (HTML, CSS and Javascript), which are then "run" inside a webview of a native app.

Ionic framework is considered the best framework for developing the a secure evoting system enhanced with mobile telephone technologies because the framework is compatible with angularjs with its associated benefits, offer better features compared to other frameworks and reduce the need for code rewriting as it provides the codes of mobile-optimized HTML, JS, and CSS components.

2.5 Implementation of a Hybrid Mobile Application (HMA)

This offers an overall construction for implementation of the HMA and tactics for improving them. These methods include development of application. More so, the software tools to be used for implementation of HMA are deliberated upon.

2.5.1 Architecture for implementing HMA

Antonelli (2006) mentions that most HMA are assembled using a three-tier or four-tier architecture. For Rashad et al (2010) suggests the use of a three- tier Client/Server architecture for web based information systems. Guynes and Windsor (2011) explains that the client/server comprises of cooperative processing abilities that physically split the processing performed by the client from that performed by the server while presenting a single logical picture to the user. Furthermore, Guynes and Windsor (2011) cite that the Client/server architecture performs a vital part in relocating large, centrally controlled applications to the smaller, distributed systems. The architecture also allow greater access to corporate data and information in addition to allowing multi-user access to shared databases.

The three–tier architecture design provides a means of structuring and disintegrating applications i.e mobile applications into three tiers of layers, where each tier provides a different level of obligation (Al-Mukhtar and Hadi, 2012). One tier is the presentation layer (user and system interfaces), another handles the business logic and the last one representing data storage (Fernandez et al, 2008; Kumar and Singh, 2010). The presentation layer contains forms or server pages which presents the user interface for the mobile application, displays the data, collects the user inputs and sends the requests to next layer (Kumar and Singh, 2010).

Business layer, which provides the support services to receive the requests for data from user tier, evaluates against business rules, passes them to the data tier and incorporates the business rules for the application.

Data layer includes data access logic, database drivers, query engines used for communicating directly with the data store of a database. Therefore, the HMA was employed using the three tier client/ server architecture.

2.5.2 Tools for implementing HMA

Hybrid development combines the best (or worst) of both the native and HTML5 worlds. Hybrid as a web app, was primarily built using HTML5, CSS and JavaScript in the ionic framework. HTML5 was designed to deliver rich content like graphics and animations or music and movies without additional plugins. Furthermore, JavaScript is needed for handling the user interface (UI) events, data transfers and different UI operations (Son et al, 2008). In addition CSS is required to make look and feel of the UI modern by telling the web browser how specific elements in the HTML file should be styled and positioned (Yemin, 2012). So, the HMA developed using HTML5 standards and can be accessed from PCs, tablets and smart phones. Java script was also used for handling UI events like validation of data entered into text fields. More so, CSS were used to improve the look and feel of the user interface (UI).

HTML5 supports the cross-platform application development i.e. designed to work whether the target platform is PC, tablet, smartphone or smart TV (Yemin, 2012). Web applications for smart phones are developed using HTML5, Java script and Cascading Style Sheets. Rashad et al (2010) propose the use of Apache as the Web Server, MySQL as the Database Server and PHP to create the Server side scripts. MYSQL is an open source database system with no licensing costs associated, and is platform independent. Furthermore, it has a high performance, scalability and security, hence making it a product widely used especially for online owned businesses (Ion-Sorin, 2011).

Maranguit et al (2011) describe PHP as an open-source general-purpose scripting language that was originally designed for web development to produce Dynamic Web Pages, but NodeJs and AngularJs were used in this case to develop a mobile application for both frontend and backend programming. Within an HTML page you can embed PHP that will be interpreted by a web server and executed each time the page loads (Welling and Thomson (2005)). Javascript, MySQL server, NodeJs, AngularJs and ionic mobile application framework were used during the development of a secure electronic voting system enhanced with mobile telephone technologies.

2.6 Software Development Life Cycle (SDLC)

According to Apoorva and Dubey (2013), a Software Development Life Cycle Model is a set of activities together with an ordering relationship between activities which if performed in a manner that satisfies the ordering relationship will produce desired software product. Software Development Life Cycle Model is an abstract representation of a development process. There are several SDLC models and a few have been listed down as follow-:

- I. Waterfall Life Cycle Model
- II. Spiral Life Cycle Model
- III. V-Shaped Life Cycle Model
- IV. Agile Life Cycle Model
- V. Prototype Life Cycle Model

2.6.1 Waterfall Life Cycle Model

Dubey and Mishra (2013) defines the waterfall model as a linear chronological software development life cycle (SDLC) model where various stages are followed such as system requirements gathering and analysis, design, coding, testing and implementation. These are presented in such a way that once a phase is over, it is not repeated again and the development does not move to next phase until and unless the previous phase is completed. Hence, the waterfall model is not very much useful when the project requirements are dynamic in nature.

In summary the waterfall model may not be applicable to this project because the system requirements in this project are dynamic in nature, and during project, it requires movement from one design phase to and from which is unacceptable in the waterfall model.

Thus, this methodology cannot be applied in designing a secure electronic voting system enhanced with mobile telephone technologies.

2.6.2 Spiral Life Cycle Model

According to Mishra and Dubey (2013) in reaction to the failures of the waterfall model argue that many new models were developed that add some form of iteration to the software development process. The spiral model has four phases: planning, risk analysis, engineering and evaluation.

A software project repeatedly passes through these phases in iterations (called Spirals in this model) (Munassar and Govardhan, 2010). The advantages of the spiral model include proper control over cost, time and manpower requirement for a project work and errors are eliminated in early phases of project development (Maheshwari and Jain, 2012). The model has high amount of risk analysis, good for large and mission-critical projects, and enables software to be produced early in the software life cycle (Maheshwari and Jain, 2012). However, the model can be expensive to use and the high risk analysis requires a specific expertise and the project's success is highly dependent on the risk analysis phase (Munassar and Govardhan, 2010). Additionally, Maheshwari and Jain (2012) emphasize that the spiral model is expensive and not suitable for smaller project since the cost of risk analysis is greater than cost of the whole project.

In conclusion, Seema and Malhotra (2012) approves that spiral software development model may be applicable to projects when creation of a prototype is appropriate, when costs are important and a medium to high-risk projects. The spiral model can also be used when users are unsure of their needs, where requirements are complex and significant changes are expected (Seema and Malhotra, 2012). This methodology could not be applied to the development of a secure electronic voting system enhanced with mobile telephone technologies since the risks of the project could not be clearly evaluated before the project.

2.6.3 V-Shaped Life Cycle Model

According to Dora and Dubey (2014) just like the waterfall model, the v-shaped life cycle is a sequential path of execution of processes. Each phase must be completed before the next phase begins. Testing is given emphasis to this model more than the waterfall model (Dora and Dubey, 2014). The testing procedures are developed early in the life cycle before coding is done during each of the phase preceding implementation. The model is simple and easy to use. Each phase has specific deliverables and there are higher chances of success over the waterfall model due to the early development of test plans during the life cycle (Munassar and Govardhan, 2010). The model works well with small projects where requirements are easily understood. However, the model has little flexibility and the adjusting scope is a problematic and costly.

Furthermore, the model does not provide a clear path for problems found during testing phases (Munassar and Govardhan, 2010). So, this model could not be applied during the development of this project which required ease in flexibility of the scope and also had unclear requirements.

2.6.4 Agile Life Cycle Model

With the popularization of waterfall-like SDLC models, an alternative approach has been developing that attempts to counter their rigidity and lack of flexibility (Mathur and Malik, 2010). The strategy for agile software development was presented by seventeen software developers, in a new attempt to bring together the best traits of other agile-like models into one framework. Since then, agile methods of development have become increasingly popular (Bhalerao et al. 2009). Another advantage of the agile model is that it is very flexible. It has been occasionally combined with other existing models. It has the capacity to deliver systems whose requirements go through constant changes while, at the same time, demanding strict time limits (Mathur and Malik, 2010).

However, agile model was not applicable in this research since more speed and lower costs involved may lead to lower overall system quality. More so, the project may end up with more requirements than needed (gold-plating).

2.6.5 Prototyping Life Cycle Model

Melissa M, et al., (2016) define prototyping as the process of building a model of a system. In terms of an information system, prototypes are employed to help system designers build an information system that intuitive and easy to manipulate for end users. Prototyping is an iterative process that is part of the analysis phase of the systems development life cycle. During the requirements determination portion of the systems analysis phase, system analysts gather information about the organization's current procedures and business processes related the proposed information system. In addition, they study the current information system, if there is one, and conduct user interviews and collect documentation. This helps the analysts develop an initial set of system requirements. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intension of being modifying or replacing it by full-scale and fully operational system (Dora and Dubey, 2014). Prototyping is an iterative process and all prototypes provide information about some aspects while ignoring others.

The designer must consider the purpose of the prototype (Houde and Hill, 1997) at each stage of the design process and choose the representation that is best suited to the current design question. Melissa, et al., (2016) suggest that prototyping can augment this process because it converts these basic, yet sometimes intangible, specifications into a tangible but limited working model of the desired information system. The user feedback gained from developing a physical system that the users can touch and see facilitates an evaluative response that the analyst can employ to modify existing requirements as well as developing new ones.

Melissa, et al., (2016) argue that prototyping comes in many forms - from low tech sketches or paper screens (Pictive) from which users and developers can paste controls and objects, to high tech operational systems using CASE (computer-aided software engineering) or fourth generation languages and everywhere in between. Many organizations use multiple prototyping tools. For example, some will use paper in the initial analysis to facilitate concrete user feedback and then later develop an operational prototype using fourth generation languages, such as Visual Basic, during the design stage.

Vijayan and Raju, (2011) point out that prototyping is one of the techniques used in requirements engineering. Instead of expensive prototypes, a throwaway paper prototype method is suggested for requirements engineering.

A paper prototype is a visual representation of what the system will look like. It can be hand drawn or created by using a graphics program. Usually paper prototype is used as part of the usability testing, where the user gets a feel of the User Interface.

Maheswari and Jain (2012) pointed out the advantages of prototyping which gives users an idea of what the final system looks like and encourages active participation among users and producer. Prototyping also enables a higher output for user, its cost effective (Development costs reduced), increases system development speed. Furthermore the model assists in identify any problems with the efficacy of earlier design, requirements analysis and coding activities. On the other hand prototyping has drawbacks which Melissa M, et al., (2016) have pointed out as follows;-

- a) Model can lead to insufficient analysis.
- b) Users expect the performance of the ultimate system to be the same as the prototype.
- c) Developers can become too attached to their prototypes
- d) Can cause systems to be left unfinished and/or implemented before they are ready.
- e) Sometimes leads to incomplete documentation.
- f) If sophisticated software prototypes (6th GL or CASE Tools) are employed, the time saving benefit of prototyping can be lost.

In summary, prototyping software development model is applicable to projects where requirements are unstable or have to be clarified to develop user interfaces and short-lived demonstrations. Methodology can as well be used for new or unique developments. Thus, it was evident that the prototyping methodology was applicable for the development of a secure electronic voting system enhanced with mobile telephone technologies since the requirements were not straight forward and hence it was applicable to this project as well. This inherently increased the amount of communication between the developer and the end user since the developer received quantifiable user feedback.

2.7 Conceptual Framework

Riggan (2012) defines conceptual framework as an analytical tool with several variations and contexts. It is used to make conceptual distinctions and organize ideas. Strong conceptual frameworks capture something real and do this in a way that is easy to remember and apply.

The conceptual framework of user-centered design was used to structure our research questions and data extraction plan, a longstanding and proven framework and methodology for the development of products, services and systems. In this framework, a user is any person who interacts with the system, service, or product for some purpose. Figure 2.2 shows a visual depiction of user-centered design, distilled from seminal work in the field of Human

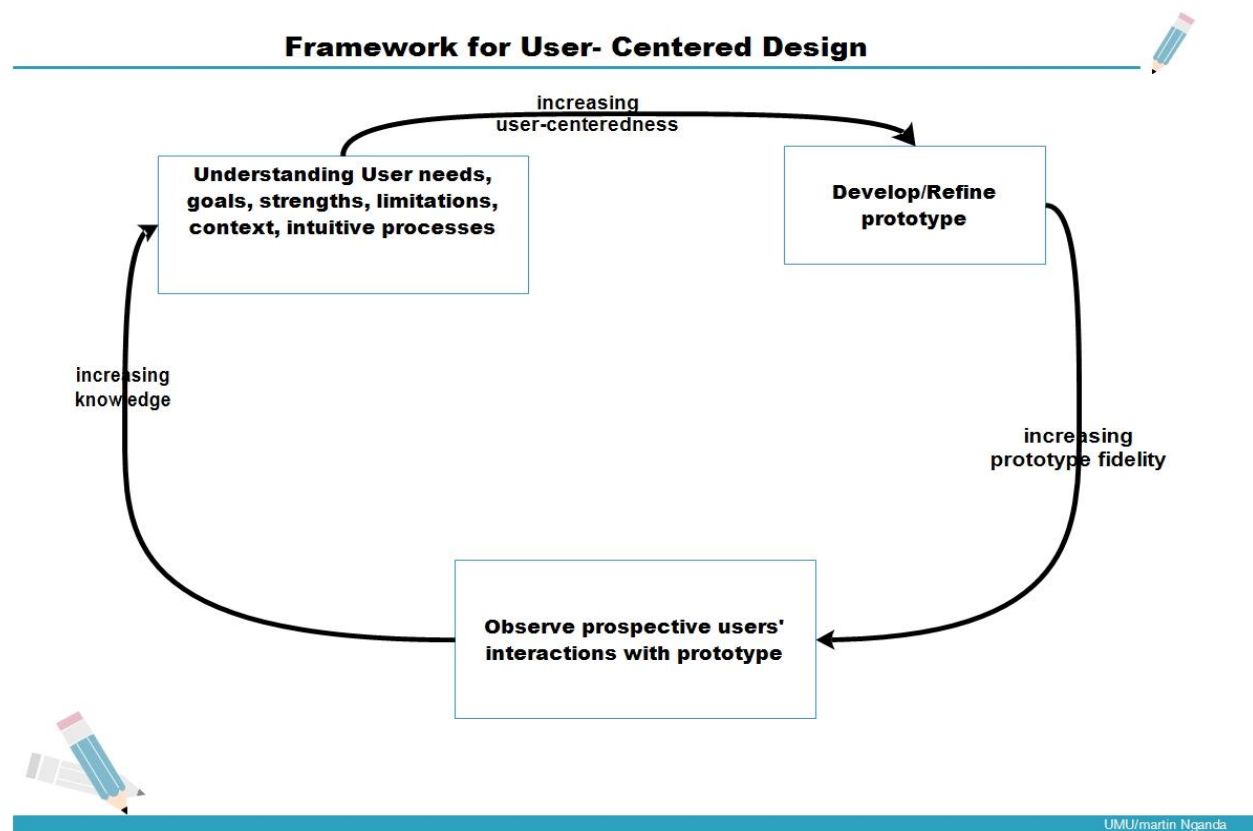


Figure 2.2: Framework for User centered Design as adopted from Witteman et al. 2015

2.7.1 User Centered Design

Usability.gov (2014) defines user centered design (UCD) as an approach that supports the entire development process with user centered activities, in order to create applications which are easy to use and are of added value to the intended users.

It is a design process that focuses on usability goals, user characteristics, user experience, environment, user tasks, and workflow. UCD follows a series of well-established techniques for the analysis, design, and evaluation of hardware, software, and a range of other interactions and device. Usabilitynet.org, (2006), claim that industry surveys have clearly shown that the majority of failed projects can be attributed to incomplete or inaccurate requirements. The biggest cost benefit that UCD can provide is by more accurately defining requirements. A design changes made late in the design process will typically cost ten times more than if identified during requirements. Making changes to working systems will cost about one hundred times more. Ideally UCD activities should be integrated with other development activities as shown in Figure

2.3. There are four important UCD principles:

- a) A clear understanding of user and task requirements
- b) Incorporating user feedback to refine requirements and design
- c) Active involvement of user to evaluate designs
- d) Integrating user centered design with other development activities

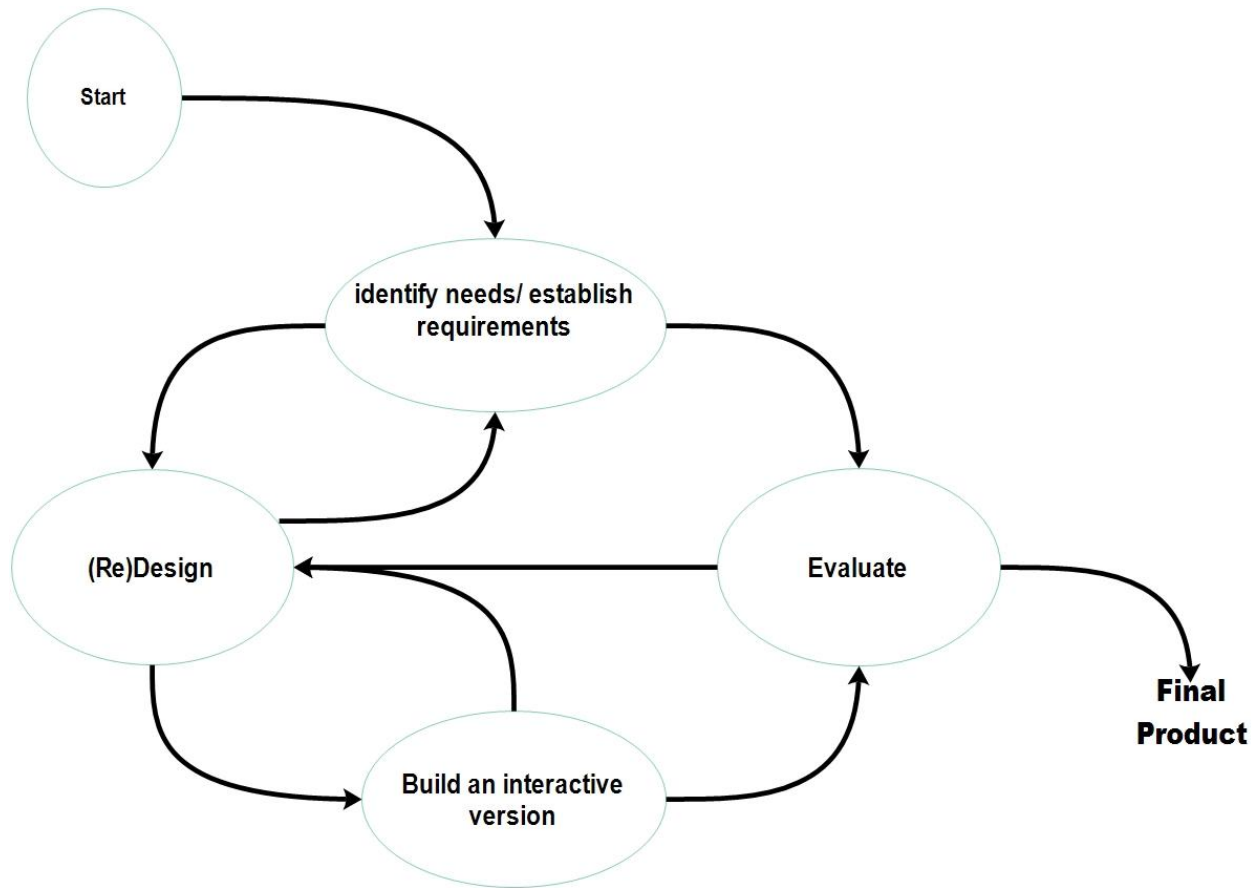


Figure 2.3: Shows the generic User Centered Design process as adopted from Rekha, 2012

In summary, UCD can be incorporated with methodologies such waterfall, agile and many other. For the success of the project, user centered design and prototyping methodology have been combined together to develop a Secure electronic voting system enhanced with mobile telephone technologies.

2.8 Conclusion

The aim of reviewing several literature in the field of IS was to find out and ensure that literature was in accordance with the main and specific objectives of the research. From the literature reviewed it was obvious that a secure electronic voting mobile app was required to improve on the quality of electoral process, minimize the time, financial and resource cost and to help the Electoral Commission to conduct their elections online and relieve them of the tedious experience that is involved with the current process.

In this research, an effort was made to develop a secure electronic voting system enhanced with mobile telephone technologies using the client/ server architecture. The Evoting system application will be installed and accessible on android smart phones.

CHAPTER THREE

METHODOLOGY

The chapter describes the various research and development methodology that was used in this project.

3.0 Introduction

This chapter comprehends the methods and tools that were used in requirements gathering and elicitation, and all the other proceeds required to achieve the objectives of this project. Specific methods were used to achieve the objectives of this project and an explanation of why such methods were used.

3.1 Research Design

A User Centered Design (UCD) approach was adopted for this project, meaning that the user was placed at the center stage in the design phase of the system developed. Usability.gov (2014) defines user centered design as an approach that supports the entire development process with user centered activities, in order to create applications which are easy to use and are of added value to the intended users. It is a design process that focuses on usability goals, user characteristics, user experience, environment, user tasks, and workflow. UCD is a broad term to describe design processes in which end-users influence how a design takes shape. It is both a broad philosophy and variety of methods. There has been limited research and debates over the use of participatory techniques in developing countries. This compelled the researcher to attempt and test this method for this project. Figure 3.1 provides a guide to the rest of this chapter.

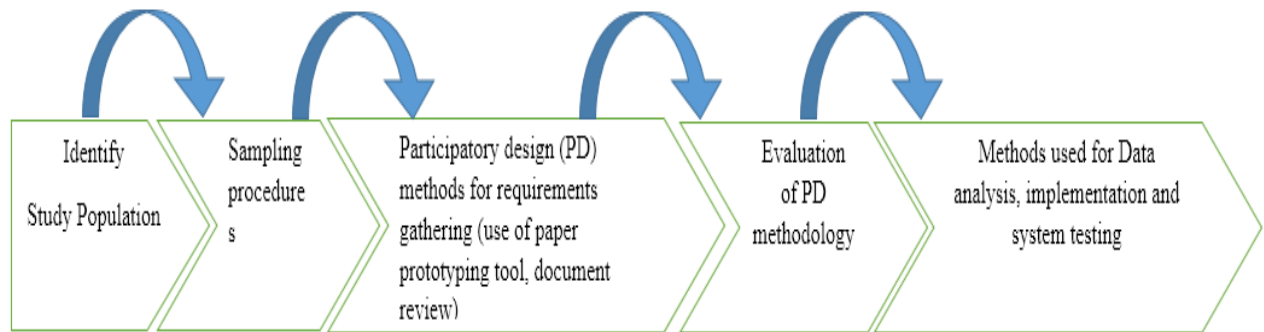


Figure 3.1: Prototyping Methodology as adopted from Usability.gov (2014)

3.2 Target Population

The researcher used Electoral commission as a case study. The research was based on a population sample encompassing of the principal election officer, and Information Technology Officers (ITOs). One principal election officer was interviewed while 10 ITOs were issued with questionnaires. This makes a total of 11 personnel. This is because 11 personnel were available and key in the management of the electronic voting system and their input was considered representative of the all the IT stakeholders for the successful implementation of the electronic voting system.

3.3 Sampling Procedures

Sampling is a practice of selecting and inquiring from a fraction of the total population for purposes of making the conclusions about the population as a whole, Oxford (2011).

3.3.1 Sampling technique

Purposive sampling was the chosen sampling technique. It is a non-probabilistic technique of sampling that gives the researcher freedom to select a sample based on judgment towards a specific purpose. This method was used by the researcher to identifying the key stakeholders who participated in the design of the system. This was made possible after a face to face interaction with the principal election officer and IT officers from Electoral commission.

3.3.2 Reasons for using this sampling technique

- a) In order to get the right information for this project, there was need to center on the key actors who actively and directly take part in the voting process. These members include principal election officer and IT officers.
- b) The sampling technique also provided for free mindedness and willingness by the respondents who were selected to participate in the entire process.

Therefore, the total sample size of the population was 11 respondents as shown in the Table 3.1 below.

Table 3.1: A Summary of the Distribution of the Sample Size

Group of respondents	Sample size
Principal Election Officer	01
IT Officers	10
Total	11

3.4 Systems Requirements Gathering and Analysis

The main objective of this stage were to document requirements for the proposed system. The researcher carried out literature review, interviews and document review during this stage. Participatory Design (PD) enables end users to become part of a design team as well as test the usability and security of systems. Analysis of results was also based on the CIA (confidentiality, integrity and availability), a famous security triangle which defines definitions and criteria that each secure system must meet. Therefore, involving users in design facilitates the elicitation of requirements and early refinements.

3.4.1 Document analysis

Useful and related sources were used in order to get the basic and necessary background about the topic. Available documentation were helpful to collect appropriate data.

The main focus of this literature studies was about the secure electronic voting systems used around the world by the electoral commissions.

3.4.2 Paper prototyping

The design phase of this project application was done with a PD by the use of paper prototyping. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intension of being modifying or replacing it by full-scale and fully operational system (Dora and Dubey, 2014). Prototyping allows the users to see and interact with a prototype allowing them to provide better and more complete feedback and specifications (Dora and Dubey, 2014). A prototype is a tangible artifact, not an abstract description that requires interpretation. Designers, as well as managers, developers, customers and end-users, can use these artifacts to envision and reflect upon the final system. On-line prototypes run on a computer and include computer animations, interactive video presentations, programs written with scripting languages, and applications developed with interface builders. Off-line prototypes do not require a computer and include paper sketches, illustrated story-boards, cardboard mock-ups and videos. The most salient characteristics of off-line prototypes (of interactive systems) is that they are created quickly, usually in the early stages of design, and they are usually thrown away when they have served their purpose. The researcher chose to use an off line paper prototype in this project. Paper prototyping is when the systems designer involves the user to sketch on a piece of paper how they intend the final product of a system should look like. It is a technique of requirements gathering that is user centered. Maria and Mattias, (2007) argue that much of the work of designers is to develop representations of design ideas and sketches contribute extensively to facilitating communication between designers and clients. In this project however, the researcher engaged the polling officials and performed several iterations using throw away paper prototypes until the prototype generated was of high fidelity which means the prototype was closer to a more refined system. A sample of 10 IT officers and 1 principal election officer were selected from the electoral commission. This reflected both a high fidelity and low fidelity of the final product. High fidelity simply means how fine or close the final product is to the sketch and a low fidelity is the reverse. Reasons for using this approach include;-

- i. Cost and time benefit: use of inexpensive material to create paper prototypes, minimum time and effort is required, Technical skills are not required to create a paper prototype.
- ii. Improved interaction between the end users and the researcher. This relieves the user of being bombarded with a product that they have to learn.

- iii. User focus: early involvement of the users in the early stage of the development lifecycle such as the conceptual review stage. This will reduce user resistance in the future.

General procedures conducted when using this method

This section describes the general procedures that were harnessed when using paper prototyping as a requirements gathering and elicitation tool.

i. Conducting an evaluation meeting.

The meeting provides a platform to debrief the stakeholders about the overall objectives of the sessions and the goals to be accomplished. The rules and guidelines on how the stakeholders were engaged when using a paper prototyping tool. The procedures that guided the researcher together with the stakeholders are summarized as:

- a) The purpose of the research, its specific objectives and their role in contributing to achieving the objectives of the research.
- b) An introductory briefing on the history of paper prototyping, its relevance and use in the industry and how it relates to participatory design.
- c) Provide participants with information about paper prototyping method as a research tool. And the free mindedness expected from them emphasizing that there is no right or wrong answer and were free to explore their creative side.
- d) Evaluation of the current system and an earlier version or competitor system to identify usability problems and obtain measures of usability as an input to usability requirements, and review of necessary documentation.
- e) Two groups are separately handled in developing the prototypes, which meant that, a number of requirements were elicited by the end of the session. All the members in each group collaboratively are tasked to develop the prototypes with the guide of the researcher.
- f) A briefing about the stationeries and materials used to develop paper prototypes. Samples of paper prototypes are provided in order to stimulate the stakeholders design.
- g) A highlight of the benefits of the prototype in order to convince skeptics and to encourage the participants to give their full commitments.
- h) Use of questionnaires

ii. Evaluation of paper prototypes

In this stage, the goal of the researcher was to conduct an evaluation in order to get the users' views and perception about the paper prototypes. This was conducted by using a table of performance measures which helped to tap the stakeholder's responses.

3.4.3 Semi-Structured Interview

The conceptual framework of user-centered design was used to structure our research questions and data extraction plan. Semi-structured interview which was used as a qualitative method for gathering data, a combination of structured and unstructured interviews. Researcher used semi-structured interview to interview both the Principal electoral officer and IT staff in response to the voting system for the reason that respondents were expected to give clarification on some of the observations which needed explanation and a perception on the prototypes generated. The researcher interviewed principal electoral officer of the electoral commission. This method was chosen because interviews provide an opportunity to explore or clarify topics in more detail. Structured interviews were conducted where the interviewee asked a standard set of questions in a particular order. All interviewees were asked the same set of questions. These questions were generated from the un-structured interview. Interviewees were selected from both operational, supervisory, management and executive levels. Each level were interviewed in two phases, the first phase was for gathering the facts and the second phase was for validating the facts gathered; thus this stage called a test-retest validity.

3.4.4 Analysis of findings

The desire to interpret the user's artifacts is necessary for purposes of system requirements acquisition, elicitation and implementation. This was done by selecting and going through the different paper prototypes and recommending the one with high precision. This exercise was conducted together with the stakeholders.

i. Data Analysis Techniques

This section explains the best fit technique that was used to analyze the data. That was extracted from the user participations.

a) Contextual and narrative analysis

Some time it was not possible to code all texts during analysis. But, contextual and narrative analysis were developed as an alternative to techniques such as coding.

Instead of segmenting the data into discrete elements and re-sorting them into categories, these approaches to analysis seek to understand the relationships between elements in particular text, situation, or sequence of events (Kaplan & Dorsey, 1991; Maxwell & Miller, n.d.). Likert scale attitude statements are utilized in order to analyze the user's satisfaction.

ii. Tools used

The Unified Modeling language (UML) was useful in collecting user requirements. After collecting this data, the system analysis and design followed in order to implement the system. The visual paradigm (UML) was useful in the design of a context diagram, EERD, and data flow diagram for the new system.

3.5 System Design

The purpose of the design phase was to plan a solution to the problem specified by the requirement document. The most important activities performed in this phase were: the design of the technical architecture and the design of system models. The primary goal of the design phase was to build a technical blueprint of how the proposed system would work, and would later be used during implementation, testing and maintenance. The design document was included information model (context diagrams) for the proposed system showing possible interactions and functionalities/modules, functional model showing design for the internal logic of each of the modules specified in context model and data model, all designed using UML language. The data model specified all the data aspects of the system such as entities involved, relationships between entities and attributes of the entities. The design models was tested and reviewed with expert evaluators, eligible voters, and research project supervisor before implementation stage.

3.6 System Implementation and Testing

The goal of the implementation phase was to translate the design of the system into code in a given programming language and testing was the major quality control measure employed during software development.

3.6.1 System Implementation

When the design was completed, major decisions about the system were made and what was left for this stage was to translate the designs of the system into code and scripts in a given programming language to implement the design in the best possible manner. During this phase, the main focus was on developing programs that were easy to write, simple, clear, and documented so as to avoid high costs of maintenance and testing. The researcher implemented the system designs basing on the security properties of confidentiality, integrity and availability of the voting system, using the Model View Controller and the following technologies;-

- a) JavaScript, a programming language used for both our frontend and backend.
- b) MySQL Server, a server hosting the database where all the data regarding different transactions are stored.
- c) NodeJs, the platform that host the backend End coding (JavaScript Code)
- d) Angular Js, used for the frontend development.
- e) Ionic, ionic is open source framework used for developing mobile applications. It provides tools and services for building mobile UI with native look and feel. Ionic framework needs native wrapper to be able to run on mobile devices.
- f) Java custom 8 step encryption algorithm with a salt combined with ionic framework for hybrid mobile application development System Testing.
- g) Advanced cryptographic techniques, end-to-end cryptographic voting techniques were used to detect integrity breaches caused from alteration of casted votes. The techniques fulfilled the voting security properties of confidentiality, integrity and availability of the new system.
- h) use of public key encryption to address data and software integrity

Testing was the major quality control measure that were deployed during development phase to detect errors in the system. During requirement analysis and design, the output was a document that was textual and non-executable. After the implementation, the goal of testing was to uncover requirement, design or coding errors in the project. The researcher deployed different levels of testing (further discussed in section 5.2). The starting point of testing was unit testing. In this a module will be tested separately and will be performed simultaneously with the coding of the module. After this the modules will be gradually integrated into subsystem, which will then be integrated and eventually form the entire system.

During integration of modules, integration testing will be performed. The goal of this testing will be to detect design errors, while focusing on testing the interconnection between modules. After the system is put together, system testing will be performed. Here the system will be tested against technical system requirements to see if all the requirements are met and the system performs as specified by the requirements. Finally, acceptance testing will be performed to demonstrate to the end users and process managers.

3.7 Deployment

The system was deployed and together with the report ready for presentation to the University panel.

3.8 Ethical Considerations

Permission to conduct this research was obtained from Electoral commission. During requirements collection, respondents were provided with enough information and voluntary participation and confidentiality of information was encouraged by the researcher. Personal identification information like names of the participants during the needs assessment meeting were keep private and confidential. Security ranks as one of the highest priorities for this study. Providing a secure and reliable system was a requirement. In this case, confidential voter detailed information is securely transmitted and accessible only by staff with the authority to view.

CHAPTER FOUR

SYSTEM DESIGN AND IMPLEMENTATION

This chapter presents findings from the data collected, analyses the results and presents the requirements gathered for the design of a secure electronic voting system enhanced with mobile telephone technologies. Evaluation of the methods used, system architecture and model were developed in this section that provided a comprehensive description of what the new system will require to achieve its objective.

4.0 Analysis of Data Collection Results

The researcher conducted a concurrent mixed study with selected key stakeholders using a purposive sampling method to implement a proper operational secure electronic voting system enhanced with mobile telephone technologies as explained in chapter three. 11 members were selected from Electoral Commission since the majority of IT staff were in the field during the time of data collection. 11 EC staff also participated as voters in the design of the new system. The researcher opted for an open approach in design and evaluation, instead of using hypothesis testing based methods to provoke inspirational responses in order to be able to automate the voting process and empowering participants to vote online using their mobile phones. Consequently, three participatory design meetings with participants were conducted where the researcher was the designer and facilitator that resulted into the development of a low to high fidelity prototypes. Table 4.0 below shows the number of participants who were engaged.

Table 4.0 showing participants from Electoral Commission

Group of respondents	Sample size
Principal Election Officer	01
IT Officers	10
Total	11

4.0.1 Results from Data Analysis.

The IT staff were asked if Information Security was an important aspect of their work.

Objective: question (1) was intended to find out the applicability of information security at EC.

The outcome of the findings were summarized as shown in Table 4.1 below.

Table 4.1: IT staff perspective on the importance of Information Security

Option	Number of participants	Percentage (%)
Strongly Agree	09	90
Agree	01	10
Disagree	00	00
Strongly Disagree	00	00
Total	10	100

The sample of the IT staff (90%) strongly agreed that Information Security was of importance to their work. Therefore, the new system was developed capable of managing confidentiality, integrity and availability of data at the Electoral Commission.

Another investigation about who is responsible for information security at the Electoral Commission was carried out.

Objective: Question (2) was to identify the end users of the new system so as to investigate and recommend secure solutions that implement information security policy and standards. Table 4.2 summarized the responses of the IT staff as shown below.

Table 4.2: In-Charge of Information security at the Electoral Commission

Option		Number of participants	Percentage (%)
IT Services		01	10
Managers and Team Leaders		08	80
Departments that use data		01	10
Individual Employees		00	00
Total		10	100

The sample of the IT staff (80%) mentioned managers and team leaders that they were the in charge of information security at EC. Therefore, the new system ensured delivery of initial security training and orientation to all IT staff, and other appropriate third parties to acquire information security management skills.

IT staff were also asked if they were aware, had read and understood the information security policy governing use of computing facilities in the commission. Question 3 and 4 were analyzed together since they shared the same objective.

Objective: To recommend use of the information security policy and apply it in the line of duty that involves addressing the security concerns of information/data at EC. Table 4.3 summarizes their responses from question 3 and 4.

Table 4.3: Information Security Policy awareness and use of computing facilities

Option: Information Security Policy and Regulation Awareness	Number of participants	Percent age (%)	Option: Information security policy and regulation governing use of computing facilities	Number of participants	Percent age (%)
Yes, I am aware	10	100	Yes, I have	10	100
No, I am not aware	00	00	No, I have not	00	00
Total	10	100	Total	10	100

The sample of the IT staff (100%) were aware of the existence of an Information Security Policy and Regulation. In addition, all the respondents (100%) had read and understood the commission information security policy and regulation governing use of computing facilities. Therefore, the new system was developed basing on the information security policy of Electoral Commission to provide general and specific guidelines to ensure that the EC’s IT resources are adequately protected. It established criteria for assigning technical access to specific IT staff including who will have access and what level of access they will be allowed

Another investigation was carried to find out if the IT staff had received awareness training on Information Security and data protection at the EC. Question 5 and 6 were analyzed together because they had the same objective.

Objective: To find out if IT staff were equipped with knowledge on data protection and information security so as to apply it in their daily tasks of safe guarding EC’s data. Table 4.5 summarized the findings of question 5 and 6 as below.

Table 4.5: Training on Information Security and Data Protection at the EC

Option: Information Security	Number of participants	Percentage (%)	Option: Data Protection	Number of participants	Percentage (%)
Yes, I have	10	100	Yes, I have	10	100
No, I have not	00	00	No, I have not	00	00
Total	10	100	Total	10	100

The all sample of the IT staff (100%) were informed on information security and data protection awareness training at the Commission. Therefore, this provided the IT staff with security mechanisms of safe guarding EC’s data. This was achieved through use of biometric mobile device and Java custom 8 step encryption algorithms for encrypting user passwords.

Another inquiry was carried out to investigate the information formats used by the IT staff.

Objective: To identify the data formats to be captured in the new system. The outcomes of the findings were summarized in Table 4.7 as shown below.

Table 4.7: Information types used by IT staff

Option	Number of participants	Percentage (%)
Voters IDs	06	60
Staff IDs or Personal Details	04	40
None of the above	00	00
Total	10	100

The sample of the IT staff (60%) were involved in voters IDs followed by 40% of the IT staff whose work involved Staff IDs captured. Therefore, the new system supported entry of new locations and voter's details.

Furthermore, the IT staff were also asked if they knew what constituted acceptable use of EC computers.

Objective: To investigate if IT staff used EC computers for their personal tasks that may compromise the electronic voting system. Tables 4.8 outlined the findings as shown below.

Table 4.8: What constitutes acceptable use of Commission computers

Option	Number of participants	Percentage (%)
I do know	10	100
I do not know	00	00
Total	10	100

All the respondents (100%) knew what was acceptable to be used on the EC's computers.

Therefore, the system supported use of EC's computers for official tasks namely; - voter's registration, voter's verification by fingerprint recognition and casting of votes. None related EC activities were not catered for in the new system.

IT staff were asked if what they did on Commission computers would affect other staff.

Objective: Question 9 was aimed at investigating the misuse of EC computers among the IT staff. The outcome of the findings were summarized in the Table 4.9 as shown below.

Table 4.9: Do EC computers affect other staff

Option	Number of participants	Percentage (%)
I agree	10	100
I disagree	00	00
Total	10	100

The sample of the IT staff (100%) agreed that what they did on commission computers would affect other staff. Computers were misused through software piracy, unauthorized access into EC databases, use of unauthorized software from home on EC computers and employees using company computers to produce materials for their own personal businesses or private use. This finding contributed to creation of user groups, rights assigned to IT staff and gained access to data authorized by EC management. Therefore, the new system proposed training of the IT staff on IT policy governing the acceptable use of EC computers.

IT staff were also asked to choose strong passwords according to the Commission Information Security Policy.

Objective: The aim of question 10 was to implement a comprehensive password policy to reduce the risk of system compromise. Table 4.10 summarized their responses as shown below.

Table 4.10: Password strength according to the Commission Information Security Policy

Option	Number of participants	Percentage (%)
\$jelF2bb	05	50
%4Btv	04	40
secret22	01	10
Administrator	00	00
Rooney	00	00
I don't know	00	00
Total	10	100

Half of the respondents (50%) recommended “\$jelF2bb” as the strongest password format because it contained a mix of letters, numbers, and symbols, followed by 40 % of the IT staff who recommended “%4Btv” password format and lastly 10 % of the IT staff chose to use “Secret22” password format. Therefore, the new system included guidelines on password construction, password security and protection standards, password aging as well as the responsibilities of users and system administrators in relation to compliance and monitoring of the policy. Additionally, no user password should be set to “never expire” and all users should be forced by the system to change their passwords periodically.

An investigation about how to secure the electoral commission computers when leaving for lunch or take a break by IT staff was carried out.

Objective: The aim of Question 11 was to investigate security controls to prevent the unauthorized access and modification to EC’s sensitive data and the use of system critical functions. Table 4.11 summarized the findings as show below.

Table 4.11: Security of computers during break time at EC

Option	Number of participants	Percentage (%)
I lock the computer	07	70
I have a password protected screensaver	03	30
I turn my monitor off	00	00
I turn the computer off	00	00
I log off	00	00
None of the above	00	00
Total	10	100

Majority of the IT staff (70%) stated that they lock the computers (Press windows key button + L) before leaving for lunch or take a break while 30% of the IT staff had password protected screensavers that denied access to intruders. Therefore, in the new system, logical access controls were deployed in assuring the confidentiality, integrity and availability of IT resources. These controls included some form of identification and authentication, access authorization, logging and reporting of user activities.

The IT staff were examined on how likely they open attachments or links that are not work related.

Objective: question 12 was to address proper use of EC email system and make users aware of what EC deems as acceptable and unacceptable use of its email system. The outcome of the findings were summarized in the Table 4.12 below.

Table 4.12: Likelihood of opening attachments / links that are not work related

Option	Number of participants	Percentage (%)
Not likely	10	100
Very likely	00	00
possibly, depending on what is being sent	00	00
Always	00	00
Total	10	100

All the respondents (100%) stated that they didn't open attachments/ links that were not work related. Therefore, the new system complied with EC email policy that email accounts should be used primarily for EC business related purposes; personal communication is permitted on a limited basis, but non EC related commercial uses are prohibited. EC email system should not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any email with this content from any EC employee should report the matter to management immediately.

Another inquiry was carried out to find out if the IT staff team shared logins and passwords. More so, the IT staff were also asked if their colleagues asked for each other's password to share so as to access the system. Question 13 and 14 were examined together because they had the same objective.

Objective: To monitor the activities of privileged users and administrators to ensure that they were not abusing or misusing their access rights. Table 4.13 and 4.14 summarized their responses as below.

Table 4.13: Share of Login Credentials

Option	Number of participants	Percentage (%)
Yes	00	00
No	10	100
Total	10	100

All the respondents (100%) indicated that they did not share logins and passwords.

Table 4.14: Sharing of passwords with colleagues

Option	Number of participants	Percentage (%)
Yes and refused to provide it	02	20
Yes and I provided it	00	00
No	08	80
Total	10	100

The majority of the IT staff (80%) stated that they have never shared for their passwords because it was captured in the information security policy and regulation that password sharing was unacceptable practice in the electoral commission. However 20% of the IT staff responded that their colleagues requested for their login credentials. Therefore, in the new system, different user groups with different user rights and privileges were uniquely assigned to each particular IT staff. Activities of all users, especially privileged users such as system administrators and all database activities were monitored and reviewed on a timely basis.

The IT staff of electoral commission were asked if they save files on the desktop or to your computer hard drive.

Objective: question 15 was to ascertain quick accessibility of EC data. The findings were summarized in the Table 4.15 below.

Table 4.15: Storage of files on the Commission computers

Option	Number of participants	Percentage (%)
Always	00	00
Sometimes	00	00
Rarely	02	20
Never	08	80
I am not sure	00	00
Total	10	100

The sample of the IT staff (20%) stated that they rarely save their files on desktop or computer hard disk however 80% of IT staff stated that they never save their files on the desktop or computer hard disk. Therefore in the new system, IT staff suggested that they prefer to save all their files on the secure centralized system not their desktops or computer's hard disk in order to protect the integrity of sensitive data.

Another investigation was carried out to ascertain which appropriate method was used by IT staff to send confidential information to another office, describe how electronic and paper documents that may contain sensitive personal information are handled in their team. Question 16 and 17 were analyzed together because they had the same objective.

Objective: To prevent confidential information from being intercepted by unauthorized persons accessing the EC networks. Table 4.16 and 4.17 summarized their findings below.

Table 4.16: Appropriate method for sending confidential information to another office

Option	Number of participants	Percentage (%)
E-mail message	00	00
Files	00	00
Hand deliver in hard copy or on USB/ CD/External Drive	00	00
Phone	00	00
Internal mail	10	100
Total	10	100

Table 4.17: Procedures for handling documents containing sensitive personal information

Option	Number of participants	Percentage (%)
Documents for internal procedures and policies to protect confidentiality	10	100
Documents are not handled in any special manner	00	00
Total	10	100

The sample of the IT staff (100%) suggested that they prefer to use internal mail to send confidential information to another office, in addition to that, all the respondents (100%) stated that all the documents are subject to internal procedures and policies to protect confidentiality.

Therefore, confidential information was accessible to only authorized EC personnel through a secure socket shell (Open SSH) in the new system. The server helped to exchange files between computer accounts or access online software archives.

Another study was carried out to investigate if the IT staff took office information home to work on with their home computers.

Objective: Question 18 was aimed at finding out whether IT staff were allowed by the information security policy to take EC information and worked on it from home with the view of submitting in assignments before the deadline.

However during document review of security policy, it was realized that IT staff were not allowed to take office work home. Table 4.18 below summarizes the findings.

Table 4.18: Use of home computers to manipulate commission information

Option	Number of participants	Percentage (%)
Almost every day	00	00
At least once a week	00	00
At least once a month	00	00
Never	10	100
Total	10	100

All the respondents (100%) responded that they have never taken information home to work on with their home computers since the information security policy did not support such acts.

In conclusion, the new system was accessible to only EC local networks within the same domain which did not allow EC data to be taken and worked on it at home.

IT staff were asked about how often they accessed commission shared drives, files, applications or emails.

Objective: Question 19 was asked to find out whether IT staff used remote services to access their applications and files. Also to identify what services were remotely accessed for the daily operations of EC. However during document review from electoral commission, it was realized that the policy had stated that remote services were accessible to IT staff. Table 4:19 summarizes the outcomes.

Table 4.19: Access to commission shared drives, files, applications or emails

Option	Number of participants	Percentage (%)
Almost every day	10	100
At least once a week	00	00
At least once a month	00	00
Never	00	00
Total	10	100

The highest percentage (100%) of staff mentioned that they accessed EC shared drives, files, applications or your emails remotely. Therefore, in the new system, remote access functionality was added in and mainly accessible to authorized IT staff for system troubleshooting purposes through private networks.

An investigation was carried out to find out whether the IT staff played a significant role in protecting office computers and the information stored on them.

Objective: To identify the IT staff that played a significant role in protecting office computers and information stored on them. Table 4.20 summarizes the outcome of the findings.

Table 4.20: Role of IT staff in protecting Office computers and information on them

Option	Number of participants	Percentage (%)
Strongly Agree	08	80
Agree	02	20
Disagree	00	00
Strongly Disagree	00	00
Total	10	100

The sample IT staff (80%) strongly agreed that they played a significant role in protecting office computers and information on them, 20% of the IT staff also agreed. Therefore, the new system emphasized use of strong privacy and authentication mechanisms to information and office computers respectively in line with user roles and permissions.

IT staff were asked if there was nothing of interest on office computers or value to others.

Objective: To identify the benefits of EC computers to IT staff daily operations. Table 4.21 summarizes the outcome as shown below

Table 4.21: IT staff interest in Office Computers

Option	Number of participants	Percentage (%)
Strongly Agree	00	00
Agree	00	00
Disagree	00	00
Strongly Disagree	10	100
Total	10	100

All IT staff (100%) strongly agreed that the office computers were of great value to the daily EC operations. Therefore in the new system, quick service delivery of IT staff was greatly achieved through use of EC computers in their daily operations like system diagnosis through research, voter registration and verification process.

More so, the IT staff were asked about their position they held at the commission.

Objective: Question 22 was intended to find out which user group interacted with the system for their daily operations so that operational roles and permissions are assigned to members of user group. The outcome was summarized in Table 4.22 below

Table 4.22: Position held by the IT staff at the Commission

Option	Number of participants	Percentage (%)
Primarily operational	10	100
Primarily administrative	00	00
Other	00	00
Total	10	100

The highest percentage (100%) of the IT staff mentioned that their positions were primarily operational, however in the new system, it was tailored to both operational and administrative tasks to cater for IT staff and their superiors (managers and commissioners).

Furthermore, the IT staff were asked to describe their titles that described their role played at the commission.

Objective: To identify the vital IT staff and their respective roles in relation to the new system.

Table 4.23 below summarized the outcome

Table 4.23: IT staff titles that describe their roles played at the commission

Option	Number of participants	Percentage (%)
Data Entrant	04	40
Data Analyst	06	60
Manager	00	00
Supervisor/ Trainer	00	00
Technician	00	00
Other	00	00
Total	10	100

Majority of the IT staff (60%) were data analysts while 40% of them were data entrants.

Therefore, the new system had a functionality that provided roles executed by both data analysts and data entrants.

An inquiry was carried out to find out how many years the IT staff had worked at the electoral commission.

Objective: Question 24 was aimed at finding out the working experience and knowledge of EC staff in electoral process since they were the key personnel in handling administrative and operational works of the system.

The summary of the outcome is given in Table 4.24 below

Table 4.24: Working experience of the IT staff at the commission

Option	Number of participants	Percentage (%)
Less than a year	00	00
Between one and three years	00	00
More than three years	10	100
Total	10	100

The sample of staff (100%) had worked at the Electoral commission for more than three years. Therefore, this implied that the IT staff had enough experience to adopt technologies of the new system.

Another investigation was carried out to find out where IT staff fall in the structure of the Electoral Commission.

Objective: The aim of the question 25 was to find out if the sample of the IT staff were all from the IT department so that they are the incharge of the new system. The outcomes were summarized in Table 4.25 below.

Table4.25: IT staff department or section at the commission

Option	Number of participants	Percentage (%)
Administration	00	00
Election management	00	00
Finance	00	00
Human Resource	00	00
Information Technology	10	100
Legal	00	00
Planning and research	00	00
Public relations	00	00
Voters data management	00	00
Total	10	100

The majority of IT staff (100%) were belonging to the Information Technology department and they proposed that other departments of EC should be incorporated into the new system.

Therefore, the new system was tailored not only to assist in the operations of the IT department but also supported operations of other departments of the electoral commission like voter verification department, public relations, administration and election management department.

IT staff were asked whether they accessed internet from their homes and the outcome is summarized in Table 4.26.

Objective: Question 26 was asked to identify which internet applications for EC are accessed by IT staff from their homes.

Table 4.26: Internet Accessibility at home

Option	Number of participants	Percentage (%)
Yes	10	100
No	00	00
Total	10	100

The Sample of the IT staff (100%) accessed internet at home.

As a result, the new system was monitored in terms of system performance using an open-source terminal emulator software called putty and Logmein application. Theses application were incorporated into the new system.

In addition, the IT staff were asked if they used social networking sites.

Objective: The aim of the question 27 was to find out if social media networking sites should be included into the new system for the IT staff. The outcome is summarized below in Table 4.27

Table 4.27: Use of Social Networking sites by IT staff

Option	Number of participants	Percentage (%)
Yes	00	00
No	10	100
Total	10	100

The Sample of the IT staff (100%) mentioned that they had no access to social networking sites since it was not allowed as stated in the Information Security policy of the electoral commission. Therefore, in the new system, IT staff proposed that social networking sites should not be catered for in the system design to comply with EC's information security policies.

4.1 System Requirements

The data collected from Electoral Commission through document review, questionnaires and oral interview helped the researcher define the system requirements which were classified into functional and non-functional system requirements.

4.1.1 Functional Requirements

The functional requirements obtained during the analysis of data collected shown in Table 4.28 below specified what the electronic voting system was supposed to accomplish.

Table 4.28: Functional requirement obtained during analysis of collected data.

Module	Functional Requirement
Administration	Allow the administrator;- <ol style="list-style-type: none"> i. add, del, edit (users, locations, polling stations, candidates, voters) ii. view results iii. upload photos and attach fingerprints for the voters iv. administer electronic voting system settings
Voting process on the mobile device	Allow the voter <ol style="list-style-type: none"> i. login with the username and password to cast the vote ii. verify the voter’s fingerprint before casting the vote (before submission) Allow the candidate <ol style="list-style-type: none"> i. login with the username and password to cast the vote ii. verify the candidate’s fingerprint before casting the vote (before submission) Allow the mobile device <ol style="list-style-type: none"> i. communicate to the database during the user fingerprint verification ii. authenticate voter’s / candidate’s credentials
Viewing results	Allow the voter <ol style="list-style-type: none"> i. View results on the dashboard. Allow the candidate <ol style="list-style-type: none"> i. view results on the dashboard

4.1.2 Non Functional Requirements

The non-functional requirements were used to identify the standards that can be applied to decide on the operation of the system, other than explicit behaviours. The system should be:

- a) easy to learn, maintain and use by its users,
- b) able to store or handle substantial and measurable volumes of data,
- c) takes optimal and minimal time to allow for efficiency when accessing or entering information and,
- d) Occupies minimal memory so as it is easily run on common operating systems, browsers and screens of changing width.

4.1.3 Software Requirements

The electronic voting web access application was developed using;-

- a) JavaScript, a programming language used for both our frontend and backend.

- b) MySQL Server, a server hosting the database where all the data regarding different transactions are stored.
- c) NodeJs, the platform that host the backend End coding (JavaScript Code)
- d) Angular Js, used for the frontend development.
- e) Java Server Faces (JSFs)
- f) Java custom 8 step encryption algorithm used to address the security properties of confidentiality, data integrity and availability system free from attacks.

The mVote and mRegister mobile applications were developed using Java and Ionic, an open source framework used for developing mobile applications for android mobile phones. These frameworks provided tools and services for building mobile user interface with native look and feel.

4.2 System Design

The electronic voting system targeted the electoral commission staff in the information technology department thus Principal IT officer, and IT officers. The diagram shown in Figure 4.1 below is general system architecture for the eVote system.

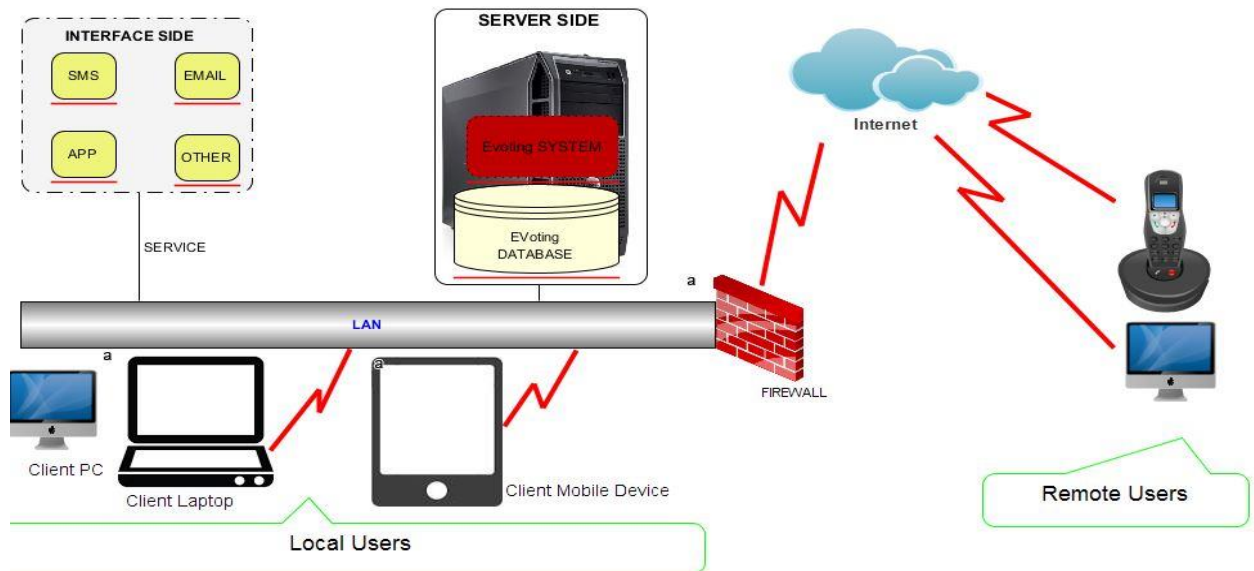


Figure 4.1: General system architecture for the eVote system

Figure 4.1 describes the overall system hardware, organization and shows the connectivity between the system components. Below are the main features of the eVote system:

Client-Server Architecture; the system is composed of server and client side to enable many users access and use the database system at the same time. The server receives requests from the users (client-side) and responds with the required service.

Local and Remote Access; users within the company local network both wired and wireless are referred to as the “Local Users” while those outside the physical location of the company are referred to as the “Remote Users”. Both Local and Remote users will have access to the same system functionality. Local Users will access the system directly whereas Remote Users will gain secure access through the firewall/proxy.

Multi-Device Access; multiple devices both portable and non-portable are supported by the system. These devices include desktop computers, laptop computers, notebooks, mobile/smart phones, personal digital assistants (PDAs), tablet computers, and etc.

Platform Independency; the EIHDMS supports a cross-section of platforms. The system will run on all devices that are running the latest major browsers such as Google Chrome, Mozilla Firefox, Internet Explorer, etc. regardless of the operating system installed on them.

Figure 4.Remote Access; remote access to the system is possible regardless of the geographical location provided internet access and with availability of VPN and/or Public IP address at the company’s center hosting the database system. Figure 4.2 below is the application technology architecture that describe the backend technologies used during the system design.

Application Technologies Architecture

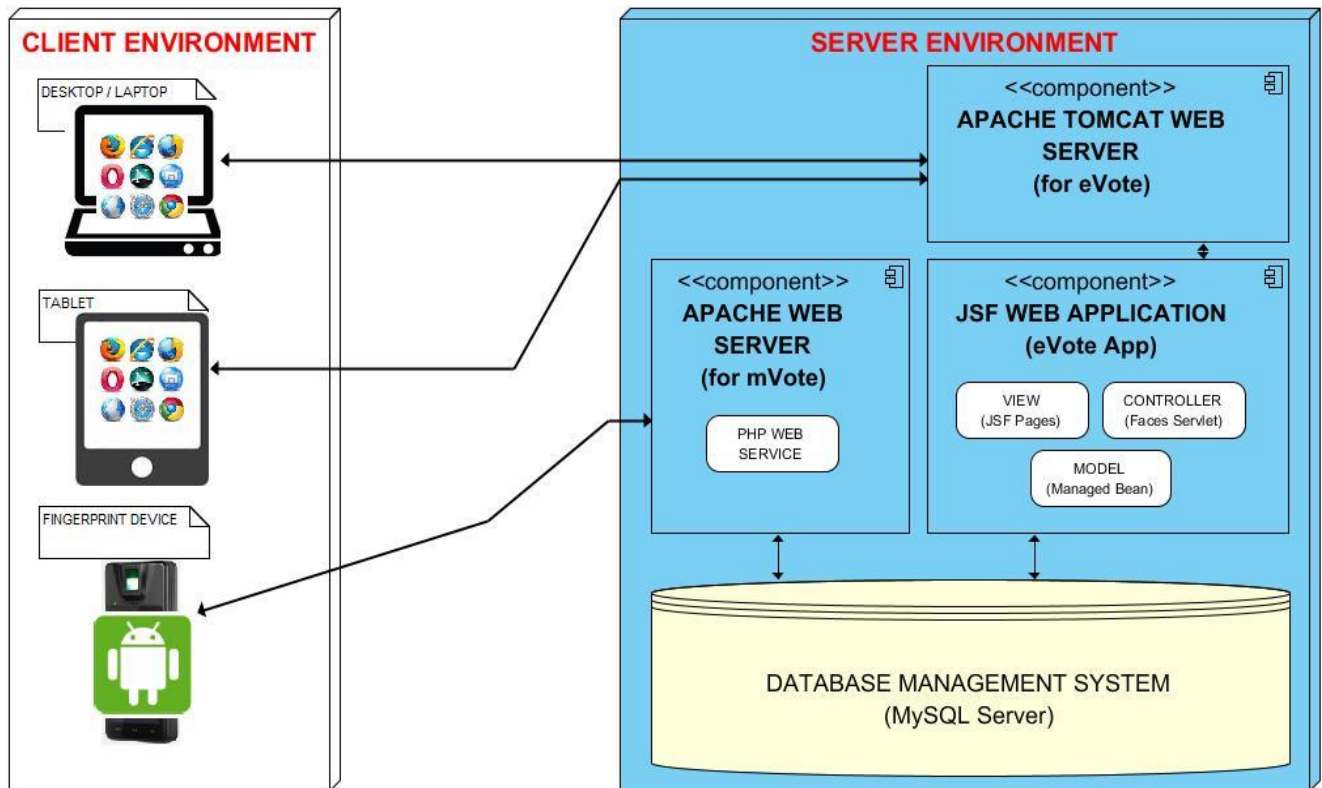


Figure 4.2: Technologies Architecture

Figure 4.2 above shows the software application technologies deployed to realize the eVote System using the Model-View-Controller (MVC) design pattern described in the literature review chapter.

Front End Applications; Oracle's Java Server Faces (Java Enterprise Edition) was used for the front-end of the system. This provides the power and flexibility needed to build user-friendly interfaces. Java Server Faces (JSF) is a Java specification for building component-based user interfaces for web applications. JSF is MVC compliant.

Back End Technologies; the open-source MySQL database Server was deployed for the backend of the system, providing a secure and robust data store.

This technology has the capability to cope with the anticipated workload, as well as allowing for expansion in the future. MySQL Server is the world's most popular open source database.

Middle Ware Technologies; Apache Tomcat was used as web server software; it is open source software and was used to implement Java Server Pages technologies. Apache Tomcat is developed in an open and participatory environment and released under the Apache License version 2. Apache Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. Apache Tomcat powers numerous large-scale, mission-critical web applications across a diverse range of industries and organizations. Figure 4.3 is showing the system architecture for android.

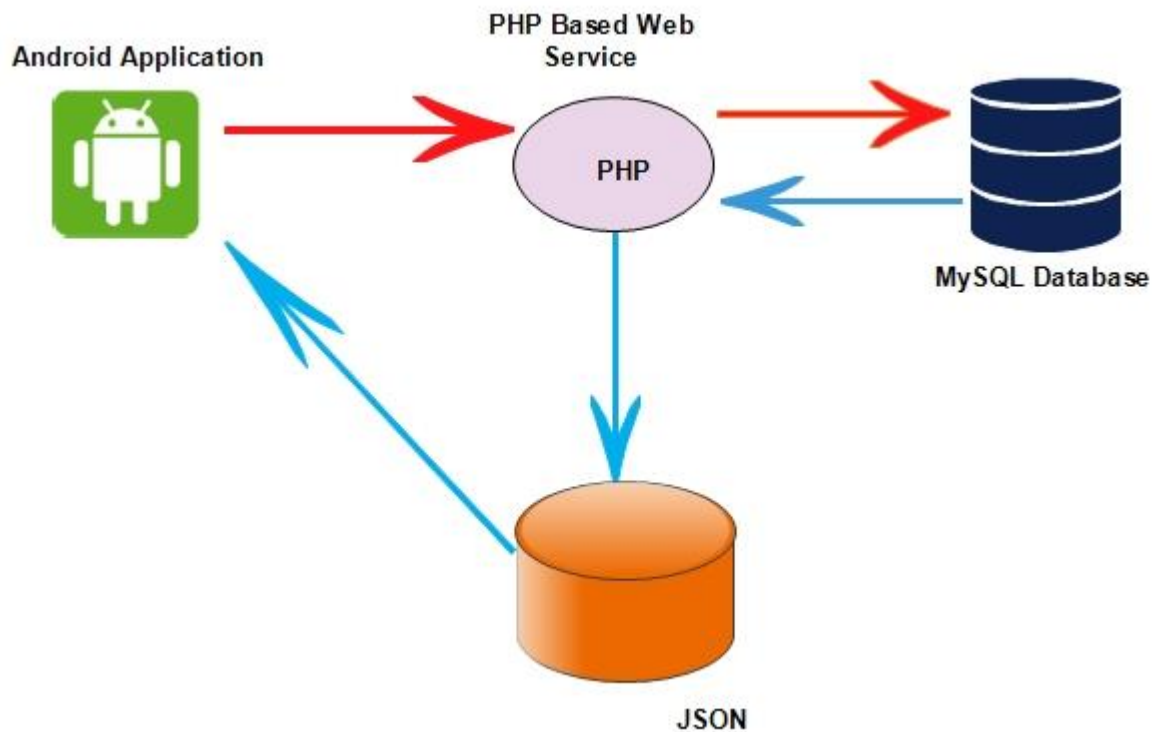


Figure 4.3: Diagram showing the Android Architecture

The android application communicates to the PHP based web service which is a bridge between the android apps and the MySQL database. JSON helps in the development of the android application for the mobile devices.

mRegister and mVote android applications function in the biometric mobile device as indicated in steps below;-

A. mRegister Application

mRegister application is applied as follows;-

i. Adding a voter’s fingerprint into the database

After capturing the fingerprint of the voter and entering their voter_id, the application sends a request to the database using the PHP service <http://mVote/communicate/registerFingerprint.php> to insert the fingerprint into the voter table for the voter whose voter_id is specified. A success/failed JSON response is returned.

B. mVote Application

mVote application is applied as follows;-

i. Verifying a voter

After capturing their fingerprint and entering their voter_id, the application does the verification of that voter by sending a request to the database using the PHP service “<http://mVote/communicate/verifyVoter.php>”. It checks whether the fingerprint matches with the one already in the database under the voter_id entered. The PHP service then returns a json object containing the details of that voter which the application displays. The voter then proceeds to cast their vote.

ii. Viewing the list of candidates

After clicking on “Click to cast Vote”, the application sends a request to the database using the PHP service “<http://mVote/communicate/getCandidates.php>”. The PHP service then returns a JSON object that contains the list of all the candidates together with their details. The application then displays this JSON object to the voter who selects a candidate of their choice.

iii. Casting a vote

When the voter clicks to cast their vote, the application sends a request to the database using the PHP service “<http://mVote/communicate/sendVote.php>” to insert the vote into the vote table. The PHP service checks whether voter_id assigned to that vote already exists in the vote table. If it doesn’t exist, it inserts the vote and then returns a success JSON response. If the voter_id already exists, a failed JSON response telling the voter that they already voted is returned.

4.2.1 Context Diagram

The context diagram was used to define the boundary between the electronic voting system and its environment showing the data communication between the system and its entities. Figure 4.4 shows the context diagram below.

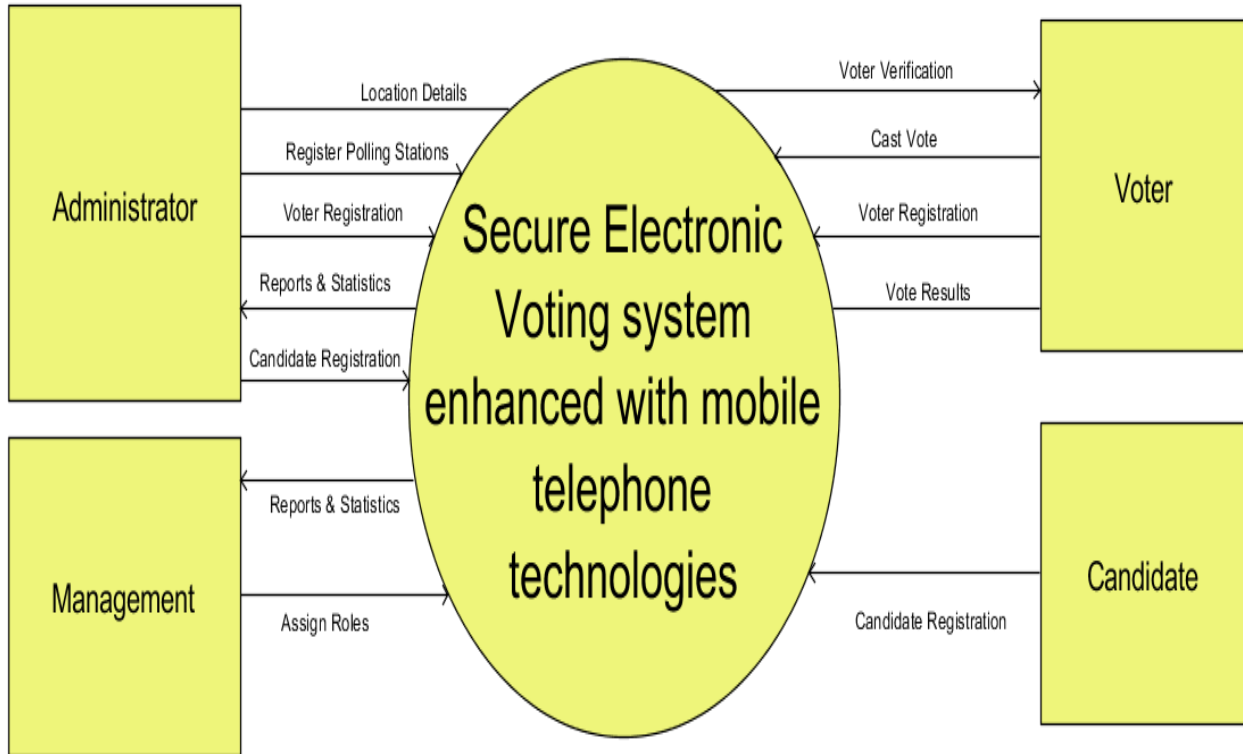


Figure 4.4: showing the context diagram

4.2.2 Dataflow Diagram

Data flow diagrams (DFD) were developed to understand the relationships between electronic voting system and its system processes, also determine if the necessary data and processes have been defined. DFDs were helpful in demonstrating how data was processed by the electronic voting system. Figure 4.5 shows the data flow diagram below.

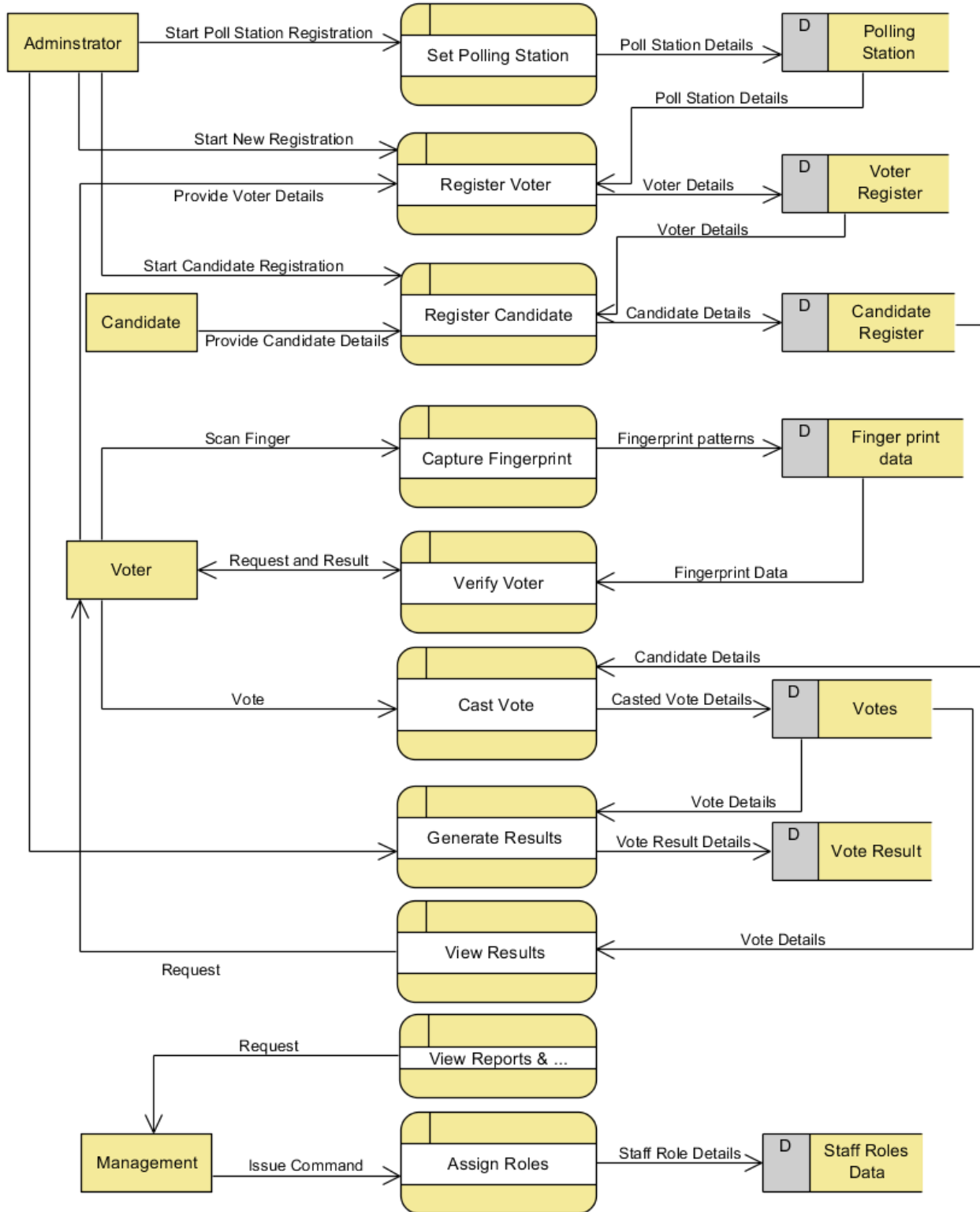


Figure 4. 5: Data flow diagrams (DFD) showing Secure Electronic Voting System

4.3 Database Design

The Database design phase was carried out to develop the required normalized table structures of the electronic voting system and the phase involved the conceptual, logical and physical database design.

4.3.1 Conceptual and Logical Design

The Enhanced Entity Relation Diagram (EERD) was precisely used to demonstrate the requirements of the electronic voting system database, show the relationships between attributes and entities. Figure 4.6 shows the EERD below.

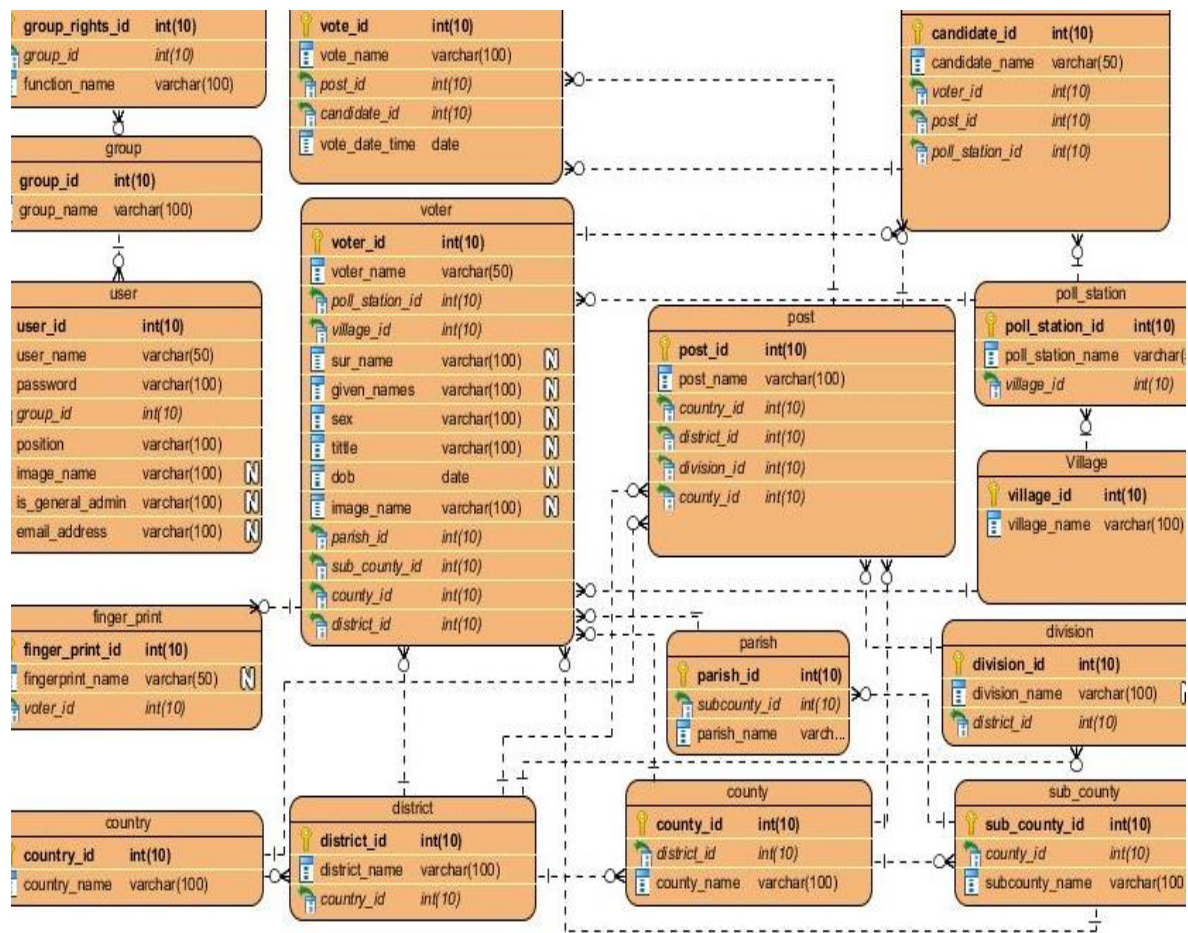


Figure 4.6: EERD for Electronic voting System

4.3.2 Physical Database Design

The physical database design involved the design of the database according to the requirements that were realized during logical modeling and also involved the conversion of the logical design into the physical design (database schemas).

Below are Normalized tables toward a secure electronic voting system with enhanced mobile telephone technologies;-

country

Column	Type	Null	Default
country_id	int(10)	No	
country_name	varchar(100)	No	
is_deleted	int(1)	Yes	NULL
is_active	int(1)	No	
add_date	datetime	Yes	NULL
add_by	int(11)	Yes	NULL
last_edit_date	datetime	Yes	NULL
last_edit_by	int(11)	Yes	NULL

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	country_id	0	A	No	

candidate

Column	Type	Null	Default	Links to
candidate_id	int(10)	No		
voter_id	int(10)	No		voter -> voter_id
post_id	int(10)	No		post -> post_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	candidate_id	6	A	No	
FKcandidate290612	BTREE	No	No	voter_id	6	A	No	
FKcandidate313655	BTREE	No	No	post_id	2	A	No	

county

Column	Type	Null	Default	Links to
county_id	int(10)	No		
district_id	int(10)	No		district -> district_id
county_name	varchar(100)	No		
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	county_id	3	A	No	
FKcounty100021	BTREE	No	No	district_id	3	A	No	

district

Column	Type	Null	Default	Links to
district_id	int(10)	No		
district_name	varchar(100)	No		
country_id	int(10)	No		country -> country_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	district_id	2	A	No	
FKdistrict112168	BTREE	No	No	country_id	2	A	No	

division

Column	Type	Null	Default	Links to
division_id	int(10)	No		
division_name	varchar(100)	Yes	NULL	
district_id	int(10)	No		district -> district_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	division_id	0	A	No	
FKdivision574007	BTREE	No	No	district_id	0	A	No	

group right

Column	Type	Null	Default	Links to
group_right_id	int(10)	No		
group_id	int(10)	No		group_detail -> group_detail_id
function_name	varchar(100)	No		
allow_view	int(1)	Yes	NULL	
allow_add	int(1)	Yes	NULL	
allow_edit	int(1)	Yes	NULL	
allow_delete	int(1)	Yes	NULL	
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	
group_detail_id	int(10)	No		group_detail -> group_detail_id

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	group_right_id	0	A	No	
FKgroup_righ766216	BTREE	No	No	group_id	0	A	No	
FKgroup_righ526408	BTREE	No	No	group_detail_id	0	A	No	

group_detail

Column	Type	Null	Default
group_detail_id	int(10)	No	
group_name	varchar(100)	No	
is_deleted	int(1)	Yes	NULL
is_active	int(1)	No	
add_date	datetime	Yes	NULL
add_by	int(11)	Yes	NULL
last_edit_date	datetime	Yes	NULL
last_edit_by	int(11)	Yes	NULL

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	group_detail_id	4	A	No	

group_user

Column	Type	Null	Default	Links to
group_user_id	int(11)	No		
user_detail_id	int(10)	No		user_detail -> user_detail_id
group_id	int(10)	No		group_detail -> group_detail_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	
group_detail_id	int(10)	No		group_detail -> group_detail_id

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	group_user_id	0	A	No	
FKgroup_user723072	BTREE	No	No	user_detail_id	0	A	No	
FKgroup_user662280	BTREE	No	No	group_id	0	A	No	
FKgroup_user902088	BTREE	No	No	group_detail_id	0	A	No	

parish

Column	Type	Null	Default	Links to
parish_id	int(10)	No		
sub_county_id	int(10)	No		sub_county -> sub_county_id
parish_name	varchar(100)	No		
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	parish_id	2	A	No	
FKparish729625	BTREE	No	No	sub_county_id	2	A	No	

polling_station

Column	Type	Null	Default	Links to
polling_station_id	int(10)	No		
poll_station_name	varchar(50)	No		
village_id	int(10)	No		village -> village_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	polling_station_id	2	A	No	
FKpolling_st7390	BTREE	No	No	village_id	2	A	No	

post

Column	Type	Null	Default	Links to
post_id	int(10)	No		
post_name	varchar(100)	No		
country_id	int(10)	No		country -> country_id
district_id	int(10)	No		district -> district_id
division_id	int(10)	No		division -> division_id
county_id	int(10)	No		county -> county_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	post_id	0	A	No	
FKpost847725	BTREE	No	No	district_id	0	A	No	
FKpost188434	BTREE	No	No	division_id	0	A	No	
FKpost626931	BTREE	No	No	country_id	0	A	No	
FKpost545044	BTREE	No	No	county_id	0	A	No	

sub_county

Column	Type	Null	Default	Links to
sub_county_id	int(10)	No		
county_id	int(10)	No		county -> county_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	
sub_county_name	varchar(100)	No		

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	sub_county_id	2	A	No	
FKsub_county278438	BTREE	No	No	county_id	2	A	No	

user_detail

Column	Type	Null	Default
user_detail_id	int(10)	No	
user_name	varchar(50)	No	
user_password	varchar(100)	No	
first_name	varchar(100)	No	
second_name	varchar(100)	No	
third_name	varchar(100)	Yes	NULL
position	varchar(100)	No	
user_image	varchar(100)	Yes	NULL
is_user_gen_admin	int(1)	No	
email_address	varchar(100)	Yes	NULL
is_deleted	int(1)	Yes	NULL
is_active	int(1)	Yes	NULL
add_date	datetime	Yes	NULL
add_by	int(11)	Yes	NULL
last_edit_date	datetime	Yes	NULL
last_edit_by	int(11)	Yes	NULL

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	user_detail_id	0	A	No	

village

Column	Type	Null	Default	Links to
village_id	int(10)	No		
village_name	varchar(100)	No		
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	
parish_id	int(10)	Yes	NULL	parish -> parish_id

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	village_id	3	A	No	
FKvillage812384	BTREE	No	No	parish_id	3	A	Yes	

vote

Column	Type	Null	Default	Links to
vote_id	int(10)	No		
post_id	int(10)	No		post -> post_id
candidate_id	int(10)	No		candidate -> candidate_id
vote_date_time	date	No		
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	
voter_id	int(10)	No		voter -> voter_id

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	vote_id	20	A	No	
FKvote351625	BTREE	No	No	post_id	2	A	No	
FKvote677075	BTREE	No	No	candidate_id	10	A	No	
FKvote252642	BTREE	No	No	voter_id	6	A	No	

voter

Column	Type	Null	Default	Links to
voter_id	int(10)	No		
polling_station_id	int(10)	No		polling_station -> polling_station_id
village_id	int(10)	No		village -> village_id
sur_name	varchar(100)	Yes	NULL	
given_names	varchar(100)	Yes	NULL	
sex	varchar(100)	Yes	NULL	
title	varchar(100)	Yes	NULL	
dob	date	Yes	NULL	
image_name	varchar(100)	Yes	NULL	
sub_county_id	int(10)	No		sub_county -> sub_county_id
county_id	int(10)	No		county -> county_id
district_id	int(10)	No		district -> district_id
is_deleted	int(1)	Yes	NULL	
is_active	int(1)	No		
add_date	datetime	Yes	NULL	
add_by	int(11)	Yes	NULL	
last_edit_date	datetime	Yes	NULL	
last_edit_by	int(11)	Yes	NULL	
parish_id	int(10)	Yes	NULL	parish -> parish_id
image_blob	longblob	Yes	NULL	
f_image	text	Yes	NULL	
f_blob	longblob	Yes	NULL	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	voter_id	5	A	No	
FKvoter537815	BTREE	No	No	polling_station_id	5	A	No	
FKvoter782752	BTREE	No	No	parish_id	2	A	Yes	
FKvoter911418	BTREE	No	No	sub_county_id	2	A	No	
FKvoter495209	BTREE	No	No	county_id	2	A	No	

4.4 Design of User Interfaces

The interface of the mRegister, mVote mobile applications and web access for administrator “<http://localhost:8080/eVoting/>” have been developed using java server faces, PHP, MYSQL Database, android application, JSON and ionic framework for mobile application development.

CHAPTER FIVE

DISCUSSION OF RESULTS

5.0 Introduction

Discussion of results involved conversion of designs into code and the physical realization of the database. It similarly involved coding the applications that will help the user to interface with the database. This chapter includes description of database implementation, implementation of user interfaces, business logic and viewing mechanisms.

5.1 System Implementation

The system implementation process included coding of the database, user interface and business logic and implementation of test plans. In the process of coding, the logical, physical design models and specifications were transformed into machine language.

5.1.1 System security implementation

During the stakeholders' meeting, users suggested that the new system be developed basing on the security requirements of Confidentiality, Integrity and Availability. Below is how each security requirement was achieved:-

Confidentiality meant keeping sensitive data secret against unauthorized users. This was achieved using cryptographic techniques like SSL and TSL in the new system. Access control also helped to grant access only to legitimate users.

Integrity is assurance of originality of data and realizing any data alteration or tampering. This was achieved through deploying logical access controls that ensured the integrity of all IT resources at the electoral commission. These controls included mechanisms of identification, authentication, access authorization, logging and reporting of user activities.

Availability is portion of time which a system must be active and available for its legitimate users. This was an important factors for preserving system availability and the capability of

failure resiliency and DoS attack counter measures. Therefore, this was achieved by providing the IT staff with security mechanisms of safe guarding EC's data which was implemented using a biometric mobile device and Java custom 8 step encryption algorithms for encrypting user passwords.

5.1.2 Database Implementation

The database and all the defined components were designed and generated using MYSQL server, the tables and their constraints namely, primary keys, unique keys, foreign keys and indices were well defined. Primary keys were used to uniquely identify all records while foreign keys were meant to ensure that data is well represented in other tables. The backend of the electronic system is accessed through

http://localhost/phpmyadmin/#PMAURL1:db_structure.php?db=wingerso_evoting&table=&server=1&target=&token=ee098431cdc2d808fd410566a72c541b. Figure 5.1 shows a screen shot of the eVote database with its tables in phpMyAdmin.

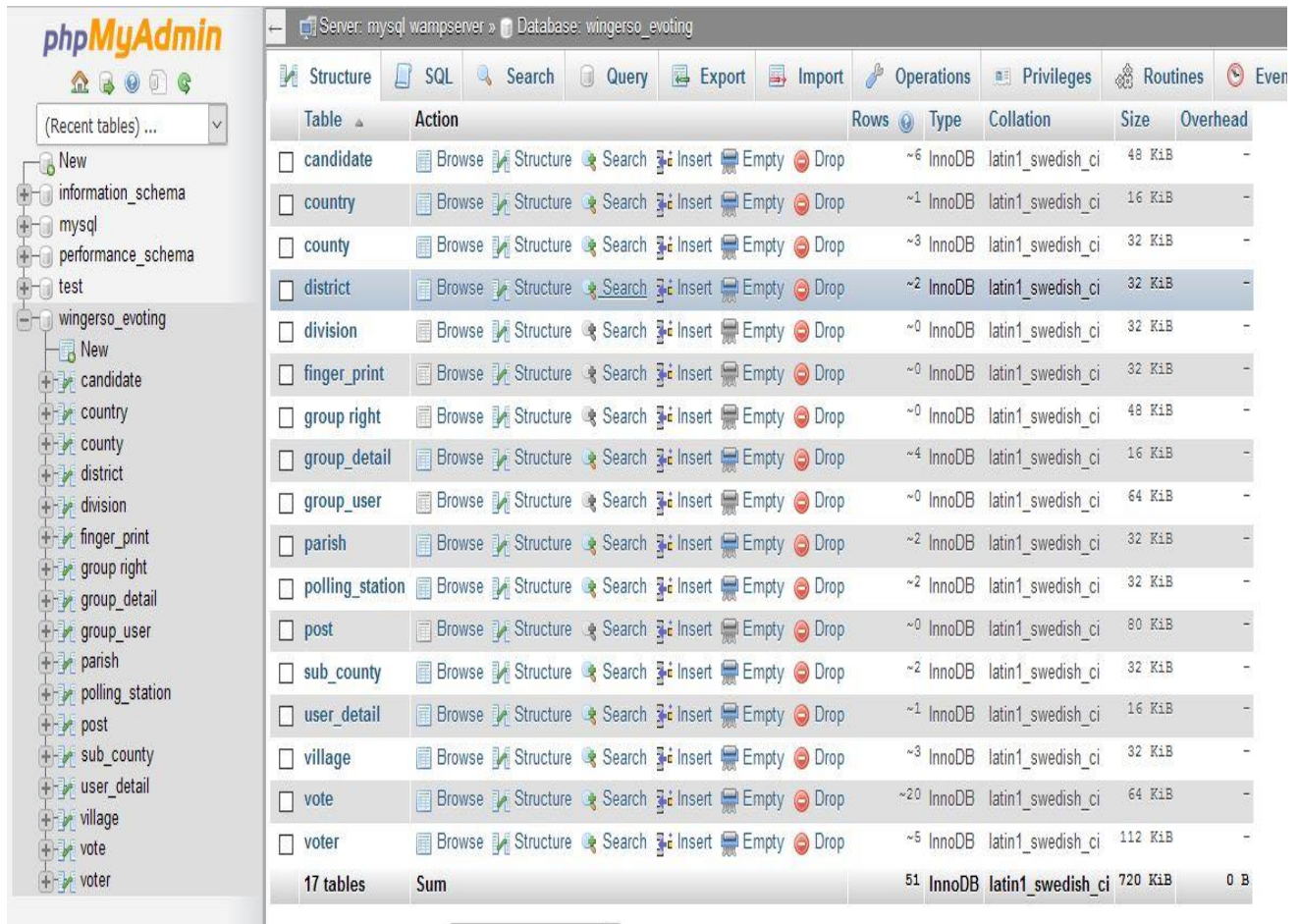


Figure 5.1: Screen shot of the eVote database with its tables in phpMyAdmin

5.1.3 Business logic and User Interfaces

The user interfaces for the voters and candidates that are viewed from the smart phones were designed by JSON, MySQL, Java Server Faces, PHP, MYSQL Database, Tomcat and Android studio framework for mobile application development. The administrator interface can be accessed using the link “<http://localhost:8080/eVoting/>”

Procedures to using the electronic evoting System;-

a) How to Register a Voter.

- i. Navigate to <http://localhost:8080/eVoting/> ;
- ii. Enter your login credentials to access the platform;

- iii. Navigate to Voter Register> Voter Details;
- iv. Enter the details of the voter ;
- v. Then click Save;
- vi. Note down the Voter ID that is assigned to that voter. This will be required by the **mRegister** and **eVote** applications to identify the voter;
- vii. Then, Open the **mRegister app** on the biometric device to capture the fingerprint of the voter;
- viii. Enter the **voter_id** already assigned to that voter, capture the fingerprint;
- ix. Then click **Register** to update the details of that voter.

b) How to Vote

- i. Open the **eVote app** on the biometric voting device;
- ii. Enter the **voter_id** and capture their fingerprint;
- iii. Click **VERIFY** for verification of that voter;
- iv. If the verification is successful, the system returns the **name** and **image** of that voter;
- v. Proceed to cast your vote.

c) How to view the results

- i. Go to <http://localhost:8080/eVoting/> ;
- ii. Navigate to View Results.

The layout of the new system as shown in figures below

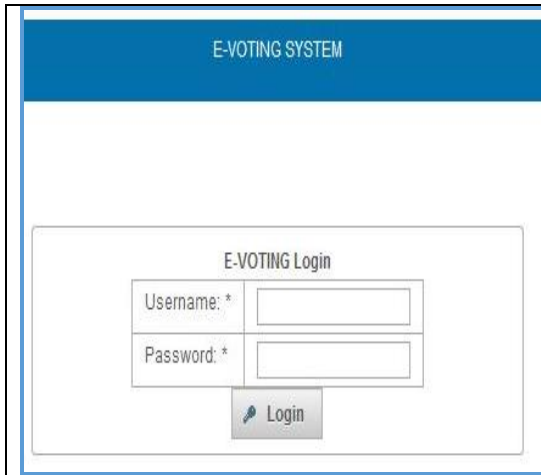


Figure 5.2: Show login interface into the eVote system



Figure 5.3: Showing how to add in a new candidate details



Figure 5.4: Showing how to add in a new voter



Figure 5.5: Showing how to capture the fingerprint of the voter using mRegister app.

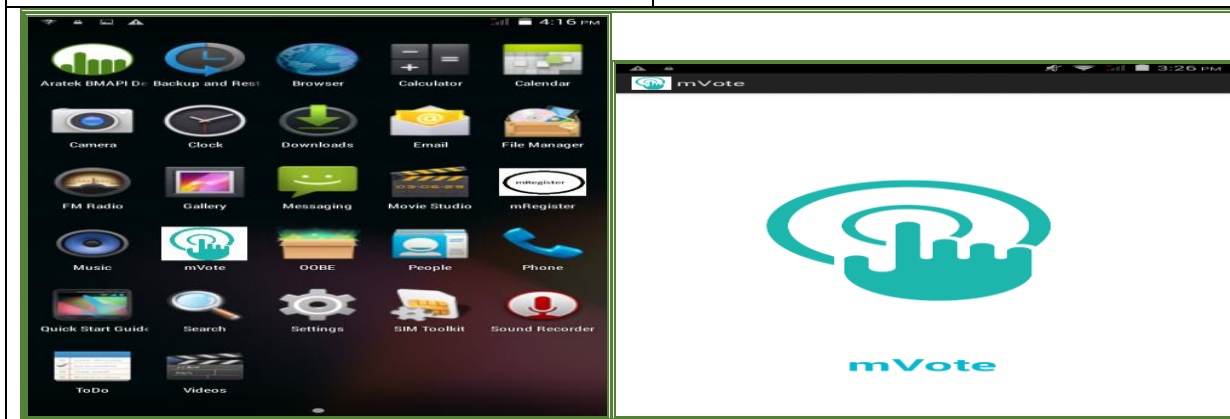


Figure 5.6: Shows the mobile interface and loading of mVote app

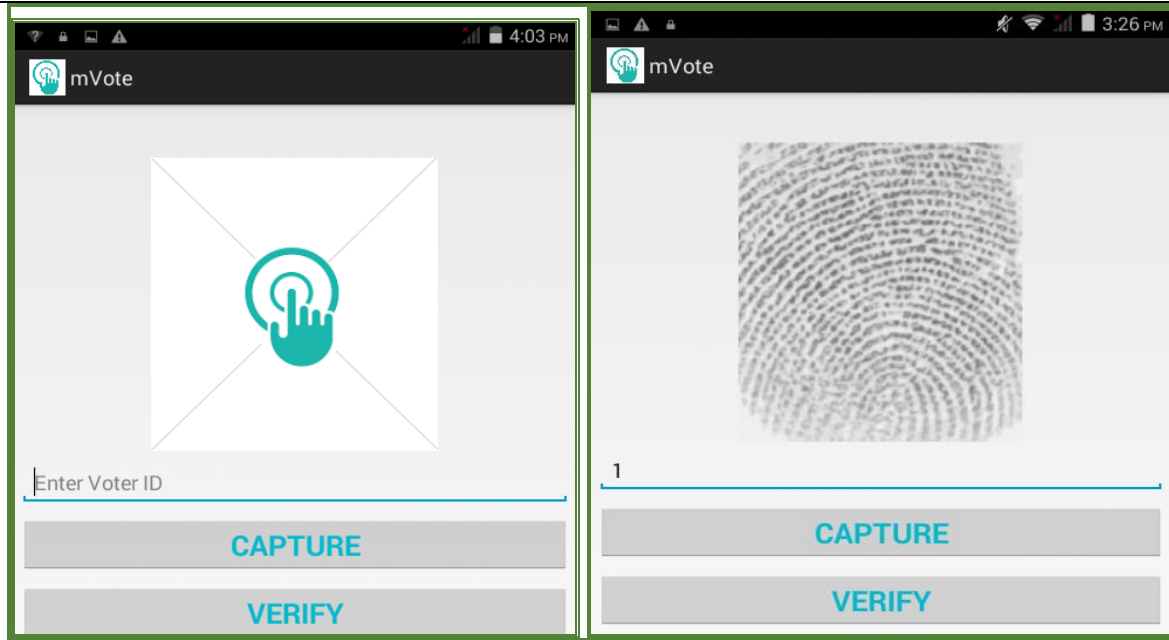


Figure 5.7: Showing verification process of voter fingerprints to access the eVote app.

During voting, the mVote application was used.

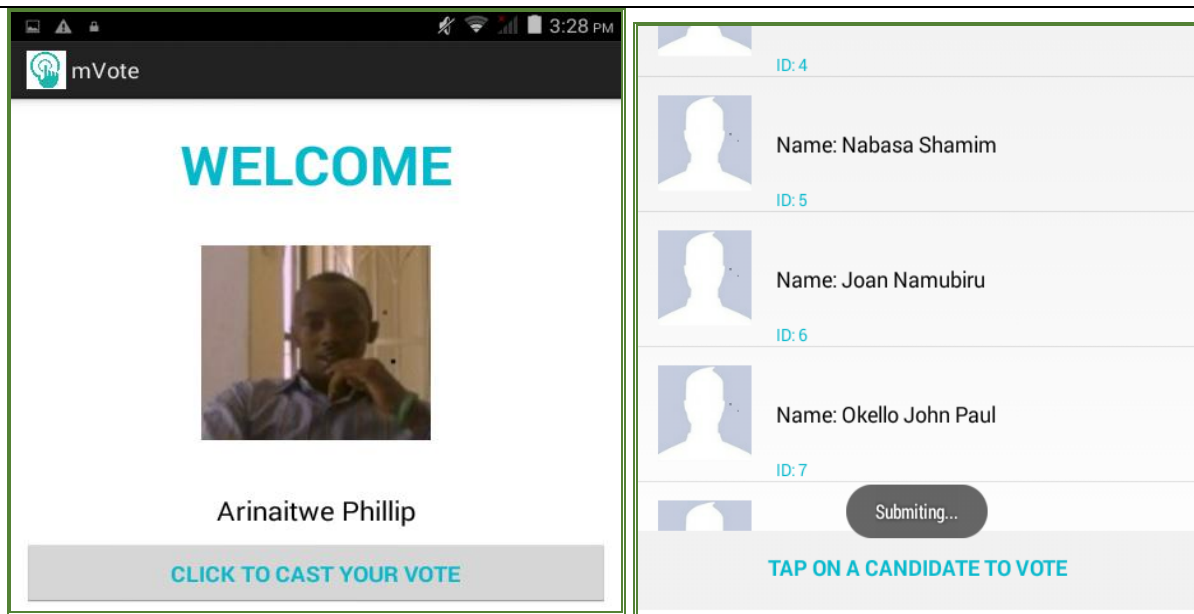


Figure 5.8: Shows casting of votes by the voter

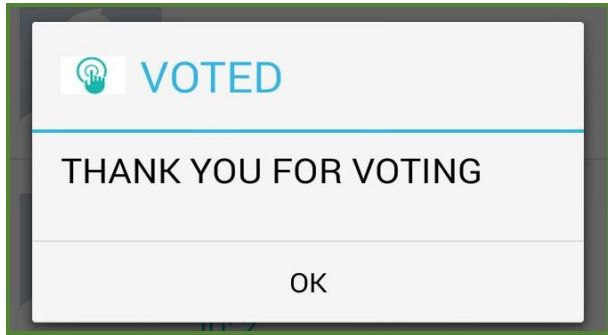


Figure 5.9: Shows submission of votes to EC servers.

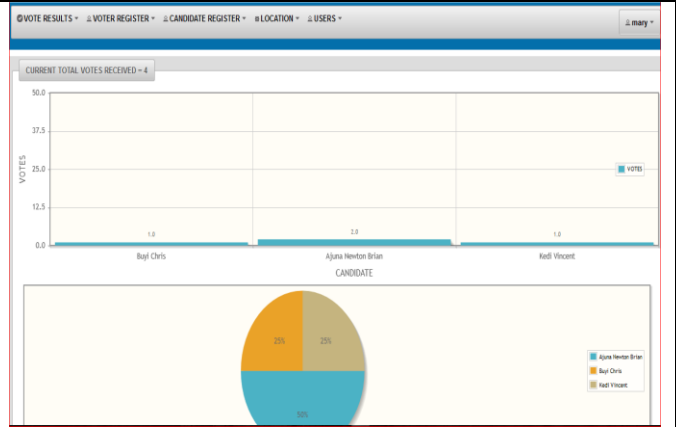


Figure 5.10: Election results from EC.

5.2 System Testing

This involved the execution of the eVote system with the emphasis of finding errors and ensuring that the system fulfills the user requirements before it was implemented. The test strategies and data were used to find system errors, database structure errors, performance requirements errors, and ensure that the system was working according to the user requirement specifications. Tables 5.1 show results of sample test cases.

Table 5.1: Tests Results

Test Classification	Test Name	Objective of test	Test Technique	Outcome
Unit Test	Creation and system maintenance of eVote accounts	To ensure that the functionality of creation and system maintenance of eVote accounts works.	Login and logout each user category to assess role assignment	Central Administrator: roles successfully assigned, Passwords created contain one digit, one lower case char, one upper case char, some special chars, length should be within 8 to 15 chars
Report test	Production of statistics from elections.	To ensure that the system can generate election statistics	Query the system for queries and compare their contents	The new system was able to show statistics from the elections accessed on http://localhost:8080/eVoting
Privacy Test	Effectiveness of password login and fingerprint recognition for user verification	To ensure that data is protected from unapproved revelation by weighing whether the system could only be accessed by users with valid log in details. Only one voter at a time was allowed by the system to cast him or her vote and one chance was given.	Fingerprint scanning during voter's verification process	System allows the voter cast vote once

Test Classification	Test Name	Objective of test	Test Technique	Outcome
Boundary Test	Response to out of range values	To ensure the system responds to unacceptable inputs.	ERs were tested but using lower and upper limit boundary values, and out of limit values (a negative value of ERs and a value greater than 100%).	A versatile system capable of handling wrong inputs and changes.
Security test	Security Measures	To ensure that the system is protected from unauthorized access.		<p>User passwords: 8 characters are accepted by the system</p> <p>Login Sessions: When one logins into the system, a session is created and destroyed at logout.</p> <p>Idle sessions are destroyed after 30seconds</p>

Table 5.2 Gives a Summary of the Tools Used in Implementation and Testing

Activity	Details	Tools Used
Coding	<ol style="list-style-type: none"> 1. Codes implementing business logic 2. Database coding 3. Statistics generation. 4. Connectivity between the database, mRegister app, eVote app and admin user interfaces 5. Connectivity between the mobile device and the database 	<p>MySQL server, PHP, Apache, Java Script, NodeJs, Angular Js, Java Server Faces and PHP, Apache, Java Script, NodeJs, Angular Js, Java Server Faces</p> <p>Tomcat 8.0 WampServer 2.0</p> <p>WampServer 2.0, Tomcat 8.0</p>
Testing	<p>Testing involved carrying out:</p> <ol style="list-style-type: none"> 1. integrity tests, 2. accuracy tests, 3. authenticity tests, 4. robustness tests, 5. mobility tests and, 6. Privacy tests. 	<p>Biometric mobile device used to authenticate voters: one person one vote,</p> <p>Results are accurately displayed at EC dashboard,</p> <p>Database is encrypted with java custom 8 encryption algorithm</p>

5.3 Discussion of Results

The main objective of the research was to implement toward a secure electronic voting system enhanced with mobile telephone technologies that provides voter's privacy, integrity, with accuracy, mobility, authenticity, non-repetition mechanism and trusted electronic voting in addition to the requirement for electronic voting. Testing was limited to module, privacy, security, integrity, accuracy and authenticity and robustness tests. From the findings of these tests, the system fully satisfied the functional, non-functional and system requirements. Therefore, it can be anticipated that research project was successful since the system fulfilled the user requirements of all the stakeholders at EC.

CHAPTER SIX

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Chapter six provides a brief summary of what has been covered with the completion of this research project. This chapter also demonstrates the challenges faced throughout the whole research undertaking together with recommendations for research in the near future on the designed system.

6.0 Summary

The key purpose of developing the system was to implement towards secure electronic voting system enhanced with mobile telephone technologies that provides voter's privacy, integrity, with accuracy, mobility, authenticity, non-repetition mechanism and trusted electronic voting in addition to the requirement for electronic voting. The research project was done in a sequence of stages. This started with identification of the problem, proposal writing and proposal defense. Later ahead, this was followed by getting hold of the introductory letter from the faculty of science for data collection which was accepted using a letter granting permission to carry out data collection from electoral commission staff.

Subsequently, data was collected using document review, questionnaires and oral interviews. The data was analyzed and requirements were drawn from this analysis. These requirements were the foundation for the system design. System modeling processes were performed using a context diagram and dataflow diagrams designed from visual paradigm version 13.2. This also involved designing the conceptual, logical and physical database design with the use of the EERD followed by normalized tables respectively. In addition, user interfaces were designed using the principals of usability, reduced user memory load and user interface consistence. These designs were a center for the operation of the prototype.

Implementation involved coding the database using phpMyAdmin and MYSQL database system, user interfaces for mRegister and mVote accessed from the mobile device were developed using JSON, MySQL, Java Server Faces, PHP, MYSQL Database, Tomcat and Android studio framework for mobile application development. Then the system was tested to ensure that it meets user requirements. The six categories of tests were done and these are the unit, privacy, integrity tests, accuracy tests, authenticity tests, and mobility tests.

6.1 Challenges

During the process of carrying out the research, the researcher encountered a number of shortcomings. These were both personal and institutional.

- a) I encountered many challenges in collecting data from the electoral commission because of the political factors involved in the organization. This led to delays to submit in my final report for the November graduation list.
- b) I also encountered a lot of challenges with the mobile device that hosted the mRegister and mVote applications due to battery failure as a result of unstable power supply. I was forced to import another mobile device from china for the success of the research project.
- c) Since I was from the BSc Ed (maths/ computer science) background, I was challenged in writing and organizing this thesis. This was because I did not undertake any research methods course unit and project at undergraduate level.

6.2 Conclusion

The design of a secure electronic voting system enhanced with mobile telephone technologies demonstrates that improving electoral process increase the quick service delivery in the electoral commission. The electronic voting system can significantly minimize the time and cost involved in the electoral process, improve data dissemination among voting participants and strengthens trust of the electoral commission to the public during service delivery.

6.3 Recommendations

For future works, as a way of improving on the security of electronic voting system, researchers should incorporate the iris scanning feature into the secure electronic voting system to cater for the handicapped population so as they participate in the voting process in the country. Alternative electronic voting methods should be provided to ensure secrecy and ease of voting across a broader range of voters with disabilities.

Confidence in the system could be further enhanced by providing a facility for open public testing of the vote recording software and the vote counting software via an on-line web interface designed to simulate the hardware interfaces of the system.

The development of an electronic register of voters can contribute significantly to the accuracy of elections: however the electronic register should remain separate from electronic voting systems in order to provide continued assurance of voter anonymity in the voting process.

REFERENCES

ADRIAN D et al (2015), <https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf>, retrieved on 13th November 2015
AGGARWAL. I AND KUMAR. V (2013), *International Journal Of Informative And Futuristic Research* Vol -1 Issue -4, December, Page No. : 41-47

ANANDA D, (2016) *The Future of E-Voting, Information, Technology and Public Policy*
<http://www.cs.washington.edu/education/courses/csep590/04au/clearedprojects/Ananda.pdf>,
retrieved on 30-05-2016

BALA, P (2015), *The advantages and disadvantages of using Ionic framework, compared to native apps*, <https://www.linkedin.com/pulse/advantages-disadvantages-using-ionic-framework-compared-pritam-bala>, retrieved on 4-06-2016

BASIE, V (2015) *Security Summit 2015*,
http://www.itweb.co.za/index.php?option=com_content&view=article&id=143438:Binney-the-NSA-is-destroying-democracy&catid=234, retrieved on 11-05-2016

BINNEY W, (2015). *Security Summit 2015*,
http://www.itweb.co.za/index.php?option=com_content&view=article&id=143438:Binney-the-NSA-is-destroying-democracy&catid=234, retrieved on 11-05-2016

BRITANNICA (2015), "*Encyclopaedia Britanica.*" <http://www.britannica.com>, retrieved on 13/10/15.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2011), *Security Considerations for Remote Electronic UOCAVA Voting (NISTIR 7770)*. United States: National Institute of Standards and Technology.

DAICHENDT L (2015), *Mobile Technology Association of Michigan*;
<http://www.strategicgrowthconcepts.com/growth/increase-productivity--profitability/mobile-technology-facts.html>, retrieved on 11-11-2015

DARIO, S (2016), *what are the advantages and disadvantages of using Ionic framework, compared to native apps?* <https://www.quora.com/What-are-the-advantages-and-disadvantages-of-using-Ionic-framework-compared-to-native-apps>, retrieved on 4-06- 2016

DIMITRIS G (2002), *Computer Security Incidents Response Teams Workshop VOL 7th* Syros, Greece <https://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf>,
retrieved on 11-11- 2015.

GARRITY EJ (2012), *Australian Article one Efficiency in the use of Information Systems*, Sydney, Australia 28(9) pp. 320 – 550.

GHEITH A., KHALID D., TAWFIQ A AND OMAR Q., (2013) "Secure national electronic voting system" *The University of Jordan, Amman* 11942, Jordan

KESSLER, G.C., (2010) “An Overview of Cryptography”
www.garykessler.net/library/crypto.html

KIM. K, AND HONG. D, (2007) “Electronic Voting System using Mobile Terminal,” *World Academy of Science, Engineering and Technology*, pp. 33-37.

MAHESHWARI, S., and JAIN, D.C., 2012. A Comparative Analysis of Different types of Models in Software Development Life Cycle. *International Journal of Advanced Research in Computer Science and Software Engineering*.2 (5).pp 285-290.

MELISSA M, LARRY R, GERRI A, (2016) what is prototyping,
<http://www.umsl.edu/~sauter/analysis/prototyping/intro.html> [Accessed on 31th May 2016]

MISHRA, A., and DUBEY, D., 2013. A Comparative Study of Different Software Development Life Cycle Models in Different Scenarios. *International Journal of Advance Research in Computer Science and Management Studies*. 1(5) pp 64-69

MOHAMMAD, J AND MORSHED, C (2013), “Comparison of e-Voting Schemes: Estonian and Norwegian Solutions”, *International Journal of Applied Information Systems* vol 6 –No.2

MOHAN A (2015) , *Password Based Encryption*,
https://web.cs.ship.edu/~cdgira/courses/CSC434/Fall2004/docs/course_docs/Article3-PBE.pdf
Accessed on 13th Nov 2015.

MOHIB ULLAH, ARIF IQBAL UMAR, NOOR UL AMIN, NIZAMUDDIN, (2013)”*An Efficient and Secure Mobile Phone Voting System*” Department of Information Technology Hazara University Mansehra Pakistan

MULALIRA, F (2016) Uganda’s legal and institutional framework in combating cybercrime, *A Review of Uganda’s ICT Law New Opportunities in the wake of recent Enactments, Old Challenges as to implementation and sensitization*.

MUNASSAR, N.M., and GOVARDHAN, A., 2010. A Comparison between Five Models of Software Engineering. *IJCSI International Journal of Computer Science Issues*.7 (5).pp 94-101.

OFORI-DWUMFUO, G. O., &PAATEY, E. 2011. The design of an electronic voting system. *Research Journal of Information Technology* 3 (2), 91-98.

OKEDIRAN O., OMIDIORA E., OLABIYISI S AND GANIYU R., (2011) “A Survey of Remote Internet Voting Vulnerabilities” ISSN: 2221-0741 Vol. 1, No. 7, 297-301,

OSKAR, W (2013) *Data Driven Development for Mobile Applications*, UPPSALA UNIVERSITET UPTEC IT 13 013Examensarbete 30 hp Augusti 2013

QIU. Y, AND ZHU. Z,(2010) “Somewhat Secure Mobile Electronic-voting Systems Based on the Cut-and-Choose Mechanism,” *International Conference on Computational Intelligence and Security*, Proc.IEEE International conference on Computational Intelligence and Security (CIS’09), vol. 1, pp. 446-450, July.

RAJ, J (2014) The Top 7 Hybrid Mobile App Frameworks, <http://ionicframework.com/>, retrieved on 4-06-2016

RAVITCH, AND RIGGAN. (2012). Reason and Rigor: *How Conceptual Frameworks guide Research*, Thousand Oaks CA: Sage p. xiii.

ROUSE M, (2016) <http://searchsecurity.techtarget.com/definition/information-security-infosec>, retrieved on 10-05- 2016

ROUSE. M (2015) <http://searchsecurity.techtarget.com/definition/security>, retrieved on 11-11-2015

SCHNEIER B (2015), https://www.schneier.com/blog/archives/2015/05/the_logjam_and_.html [Accessed on 13th November 2015]

SEEMA and MALHOTRA, S (2012). Analysis and tabular comparison of popular SDLC models. *International journal of advances in Computing and Information Technology*.

SEKAGGYA M (2010), “*Management of Elections in Uganda*” The Open Society Initiative for Eastern Africa.

SHAUN H, AND CHOUDHRAY. A, (2011) “Intelligent Polling System Using GSM Technology,” *International Journal of Engineering Science*, vol. 3

STALLING, W., (2003) *Cryptography and Network Security*, 3rd Edition, Prentice Hall, New Jersey.

SWADDLE P, (2016) Mobile technology trends in 2016 – *More about evolution than revolution*, <http://www.itproportal.com/2016/02/01/mobile-technology-trends-2016-more-evolution-than-revolution/#ixzz48X7w1Cwu> [Accessed on 14th May 2016]

TWESIGYE G, (2013), “Presentation to East African Information Security Conference” *Top IT Security risks and challenges*.

USABILITY.GOV (2014) <http://www.usability.gov/what-and-why/user-centered-design.html> [Accessed on 14th June 2016]

VÍCTOR MATEU, FRANCESC SEBÉ, AND MAGDA VALLS, (2013) *Journal of Network and Computer Applications* 42 (2014) 39–44

VIJAYAN, J AND RAJU, G, (2011) A New approach to Requirements Elicitation Using Paper Prototype.

WILLIAM W, (2016) *Global Forum for Cyber Expertise Awareness Initiative*
<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/8.-symantec-corporation-gfce-cybersecurity-and-cybercrimetrend-in-africa-initiative.pdf>, [Accessed on 12th May, 2016]

WITTEMAN et al. (2015) *Systematic Reviews*,
<http://www.systematicreviewsjournal.com/content/4/1/11>

ZWASS V (2016), Information System. <http://www.britannica.com/topic/information-system>
[Accessed on 11th May 2016]

APPENDICES

Appendix 1A

Information Security Awareness Questionnaire for Information Technology Staff

Dear Participant,

My name is Martin Nganda, currently doing a Master of Science Degree in Information Systems at Uganda Martyrs University. My research thesis for the fulfillment of the degree is titled; **“TOWARDS A SECURE ELECTRONIC VOTING SYSTEM ENHANCED WITH MOBILE TELEPHONE TECHNOLOGIES”**. Please by completion of the attached questionnaire, your input and time will be of great importance towards developing a secure electronic-based voting system for Uganda. All information provided will be treated with strict confidentiality. Please give me your insight. I am exploring the level of Information Security Awareness in Electoral Commission IT staff.

Because we are talking about security, some of the questions may read as if I am trying to catch you out. This is not the case. There are no right or wrong answers – I am looking for honest insight. Remember, your individual responses will remain confidential.

Thank You.

Security Responsibilities

1. Information Security is an important part of my work
 Strongly Agree Agree Disagree Strongly Disagree
2. Who is responsible for information security at the Electoral Commission (select all which apply)
 IT Services Departments that use data
 Managers and Team Leaders Individual Employees
3. Are you aware of the existence of an Information Security Policy and Regulation Governing Use of Computing Facilities in the Commission
 Yes, I am aware No, I am not aware
4. Have you read and understood the Commission Information Security Policy and Regulation Governing Use of Computing Facilities
 Yes, I have No, I have not

5. Have you received Information Security awareness training at the Commission
 Yes, I have No, I have not
6. Have you received Data Protection awareness training at the Commission
 Yes, I have No, I have not
7. Does your work involve any of the following information types? (select all which apply)
- | | |
|---|--|
| <input type="checkbox"/> Voters IDs or Personal Details | <input type="checkbox"/> Staff IDs or Personal Details |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Research Information |
| <input type="checkbox"/> None of the above | |

Using Electoral Commission computers

8. Do you know what constitutes acceptable use of Commission computers
 I do know I do not know
9. What you do on Commission computers could affect other staff
 I agree I disagree
10. Passwords are important for preventing unauthorized access to information. Which of the following are strong passwords according to the Commission Information Security Policy? (select all which apply)
- | | | |
|--|------------------------------------|---------------------------------------|
| <input type="checkbox"/> Administrator | <input type="checkbox"/> \$jelF2bb | <input type="checkbox"/> %4Btv |
| <input type="checkbox"/> Rooney | <input type="checkbox"/> secret22 | <input type="checkbox"/> I don't know |
11. When leaving for lunch or to take a break, how do you secure your computer?
- | | | |
|--|--|--|
| <input type="checkbox"/> I turn my monitor off | <input type="checkbox"/> I log off | <input type="checkbox"/> I lock the computer |
| <input type="checkbox"/> I turn the computer off | <input type="checkbox"/> I have a password protected screensaver | |
| <input type="checkbox"/> None of the above | | |
12. If someone e-mails you an attachment/link that is not work related, how likely are you to open it?
- | | |
|-----------------------------------|---|
| <input type="radio"/> Not likely | <input type="radio"/> possibly, depending on what is being sent |
| <input type="radio"/> Very likely | <input type="radio"/> Always |

13. Does your team share logins and passwords?
 Yes No
14. Has anyone you know at work asked for your password?
 Yes and I provided it Yes and refused to provide it No
15. Do you save files to the desktop or to your computer's hard drive
 Always Sometimes Rarely Never I am not sure

Handling Information

16. You are asked to provide confidential information to another office. What is an appropriate method for sending this information? (select all which apply)
 E-mail message Files. Phone
 Hand deliver in hard copy or on USB/ CD/External Drive Internal mail
17. Electronic and paper documents may contain sensitive personal information. Which statement best describes how these documents are handled in your team? *
 Documents are not handled in any special manner
 Documents are subject to internal procedures and policies to protect confidentiality
18. How often do you take information home to work on with your home computer?
 Almost every day At least once a week
 At least once a month Never
19. How often do you access Commission shared drives, files, applications or your emails remotely?
 Almost every day At least once a week
 At least once a month Never
20. You play a significant role in protecting your office computer and the information stored on it
 Strongly Agree Agree Disagree Strongly Disagree

21. There is nothing on your office computer that would be of any interest or value to others
 Strongly Agree Agree Disagree Strongly Disagree

About You. Please remember, this questionnaire is to inform our understanding of information security awareness at the Commission. It is by no means a test.

22. Is your position
 Primarily operational Primarily administrative Other

23. Which of the following title comes closest to describing your role? *
 Data Entrant Data Analyst Manager
 Supervisor/ Trainer Technician Other

24. How many years have you worked at the Commission?
 Less than a year Between one and three years More than three years

25. Which is your Department and Section

26. Do you access the internet from home?
 Yes No

27. Do you use social networking sites?
 Yes NO

Thank you very much for your time

Appendix 1B

Information Security Assessment Oral Interview

Interviewee: System Administrator/ IT Technical Staff – Uganda Electoral Commission Head Office

Date:

My name is Martin Nganda, currently doing a Master of Science Degree in Information Systems at Uganda Martyrs University. My research thesis for the fulfillment of the degree is titled; **“TOWARDS A SECURE ELECTRONIC VOTING SYSTEM ENHANCED WITH MOBILE TELEPHONE TECHNOLOGIES”**. Please by answering my questions your input and time will be of great importance towards developing a secure electronic-based voting system for Uganda. All information provided will be treated with strict confidentiality.

Basic Information

Does the Commission have an Information Technology policy document and regulations	
If the Commission has an Information Technology policy document and regulations is the IT staff given the document and trained about it during orientation	
How many Computers were used to process 2016 elections	
How many Servers were used to process 2016 elections	
Please explain how data moves from the polling centre up to when it becomes election results	

Audit Information

Do you audit computer system use in the Commission? If so how is the audit carried out	
--	--

Network Security Information

Has your organization ever been compromised internally - If so give details	
Has your organization ever been compromised externally - If so give details	
Are you aware of IP address blocks registered to your organization. (Example – 12.34.56.x/24)	
Are you aware of all the domain names registered to your organization?	

Does your organization use a local Firewall(s) If so, please list quantity and manufacturer(s) of firewall(s).	
Does your organization use a local Intrusion Detection System(s) (IDS)	
Does your organization use a local Intrusion Prevention System(s) (IPS)	
If your organization uses local IDS, do you use “host-based” IDS (HIDS) or “network-based” IDS (NIDS) or a combination of both?	
Do you use DMZ networks	
Does your organization have any dedicated connections to other organization’s networks (vendors, business partners)?	
Does your organization use any Remote Access services? Specifically, what type of remote access services does your organization use (VPN or Dial-Up RAS)?	
How many employees use remote access services?	
Does your organization use site-to-site Virtual Private Network (VPN) tunnels? If so, how many site-to-site VPN tunnels are in use?	
Does your organization have any systems that use modems?	

System Information

Does the Commission use Microsoft Windows servers ?	
Does the Commission use Unix servers (AIX, HPUX, Linux, Solaris, etc.)	
Does the Commission use servers with operating systems other than Microsoft Windows and Unix servers	
Does the Commission use any Enterprise Resource Planning (ERP) application(s)? (Examples – SAP, Peoplesoft, Oracle, JD Edwards)	
Does your organization use E-commerce application(s)?	

<p>What database technologies does your organization use? (Examples – Oracle, Microsoft SQL, IBM DB2, MySQL)</p> <p>Please give a brief description of the purpose for each.</p>	
--	--

Service Information

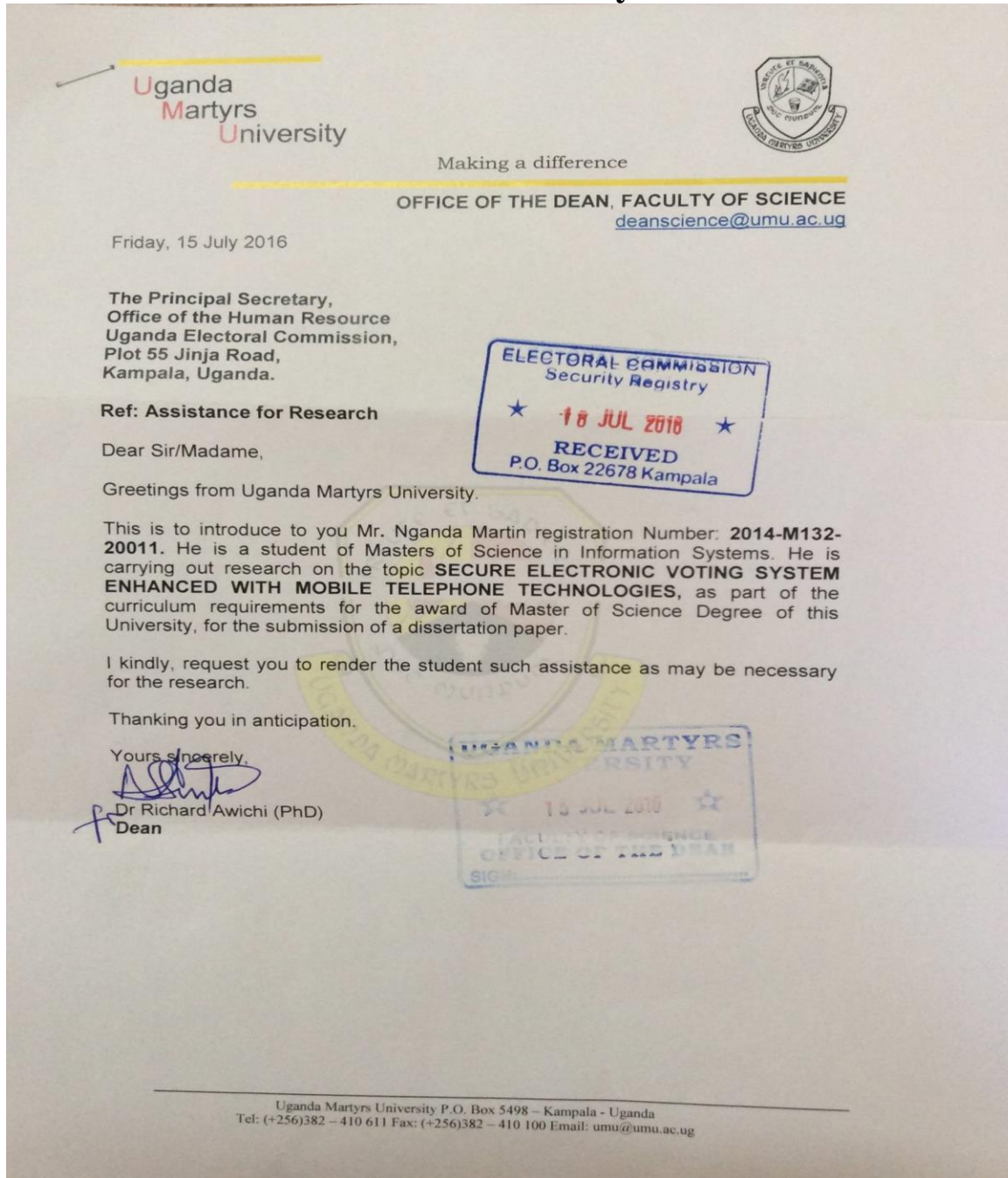
<p>What services do you expose to the internet? (Examples: Web, Database, FTP, SSH, etc.)</p>	
<p>What services do you expose to the Electoral Commission staff?</p>	
<p>What type of authentication do you use for your web services? (Examples: PubCookie, Windows Integrated, htaccess, etc.)</p>	
<p>What languages do you use for your web services? (Examples: PHP etc)</p>	
<p>What antivirus application(s) do you use?</p>	
<p>Is your antivirus application implemented using a “managed” client/server architecture, or in a stand-alone configuration?</p>	
<p>How often do you update the antivirus application(s)</p>	

Any other information you would like to add on?

Thank very much for your time

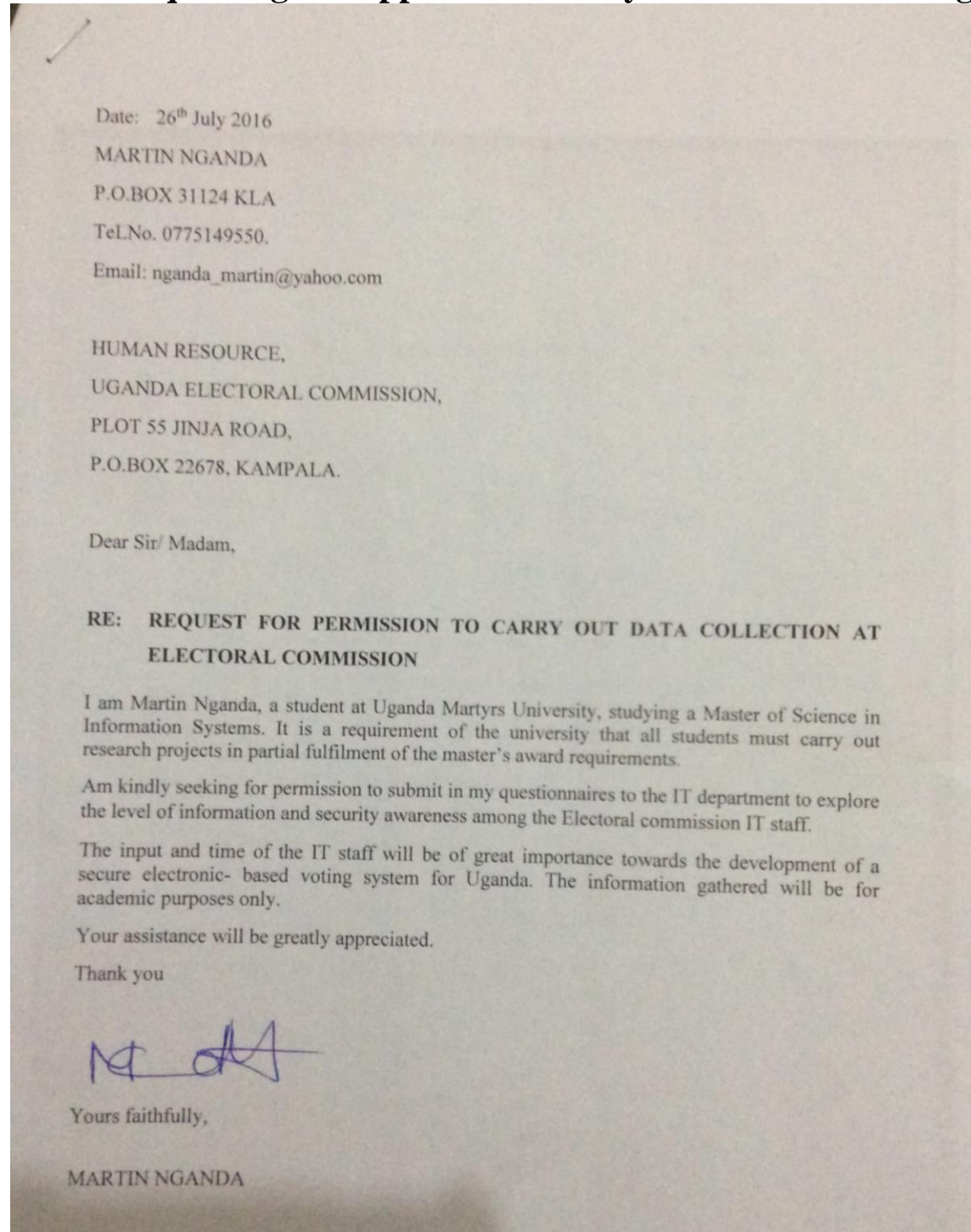
Appendix 2A

Letter of Introduction from the Faculty of Science of UMU



Appendix 2B


Letter Requesting for Approval to Carryout Research Findings



Appendix 2C

Authorization Letter for the Researcher To Carryout Research

THE REPUBLIC OF UGANDA
THE ELECTORAL COMMISSION



Telephone: +256-41-337500/337508-11
Fax: +256-31-262207/41-337595/6
E-mail: secretary@ec.or.ug

Plot 55 Jinja Road
P. O. Box 22678 Kampala, Uganda
Website: www.ec.or.ug

Our Ref: **ADM/82/01** Date: **July 29th, 2016**

Mr Martin Nganda,
P. O. Box 5498,
Uganda Martyrs University,
KAMPALA
Tel; **0775149550/0703449444**

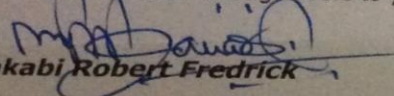
Dear Sir,

RE: **RESEARCH AT THE COMMISSION**

We acknowledge receipt of your application dated 15th July 2016 requesting to carry out research in our Institution.

This is to inform you that your request has been considered and you have been offered an opportunity to carry out the said research at the Electoral Commission in **Information Technology Department** on condition that the research process and report will be exclusively used for academic purposes and upon swearing that you will not divulge information from the Commission without the written consent of the Secretary, Electoral Commission.

The period of your research is from **29th July to 29th August 2016**. Therefore, you should report to the undersigned for further guidance if the offer and conditions therein are agreeable to you.


Wakabi Robert Fredrick

For: **SECRETARY, ELECTORAL COMMISSION**

c.c. H/IT