



**A CONCEPTUAL MODEL FOR DESIGNING AND IMPLEMENTATION
OF SECURE AND TRUSTABLE REMOTE ELECTRONIC VOTING SYSTEMS
WITHIN THE DEVELOPING WORLD**

By

LAPOLOGANG NTWAYAME

Reg. No: 14100552

BSc (Computer Software Engineering) (SU), MSc (Information Systems) (BIUST)

Department of Computer Science and Information Systems,
College of Science,
Botswana International University of Science and Technology,
Student E-mail address: lapologang.ntwayame@studentmail.biust.ac.bw
Tel: (+267) 76608641/73335734

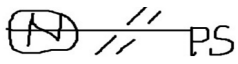
A Dissertation Submitted to the College of Science in Partial Fulfillment of the Requirements
for the Award of the Degree of Master of Science in Information Systems of BIUST

Supervisor(s): Dr. Malatsi Galani

Department of Computer Science and Information Systems,
College of Science, BIUST

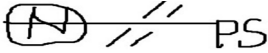
E-mail Address: galanim@biust.ac.bw

Phone Number: (+267) 4931106

Signature:  PS Date: 28/04/2018

DECLARATION AND COPYRIGHT

I, **Lapologang Ntwayame**, declare that this dissertation is my own original work and that it has not been presented and will not be presented to any other university for a similar or any other degree award.

Signature:  _____

This dissertation is copyright material protected under the Berne Convention, the Copyright Act of 1999 and other international and national enactments, in that behalf, on intellectual property. It must not be reproduced by any means, in full or in part, except for short extracts in fair dealing; for researcher private study, critical scholarly review or discourse with an acknowledgment, without the written permission of the office of the Provost, on behalf of both the author and the BIUST.

CERTIFICATION

The undersigned certifies that he has read and hereby recommends for acceptance by the College of Science a dissertation titled: **A CONCEPTUAL MODEL FOR DESIGNING AND IMPLEMENTATION OF SECURE AND TRUSTABLE REMOTE ELECTRONICVOTING SYSTEMS WITHIN THE DEVELOPING WORLD**, in fulfilment of the requirements for the degree of Master of Science (Information Systems) of the BIUST.



Dr.MalatsiGalani
(Supervisor)

Date: 28/04/2018

ACKNOWLEDGEMENTS

This dissertation is the outcome of hard work conducted at Botswana International University of Science and Technology (BIUST), College of Science and Department of Information Systems and Computer Science. I would like to thank Prof. Irina Zlotnikova and Dr. Malatsi Galani for their efforts and encouragement towards fulfilling this goal, without their intervention none of this work would have been possible.

I would also like to pass my appreciations to my mentors Dr. Dimane Mpoeleng, Dr. Rajalakshmi Selvaraj and Dr. Hlomani Hlomani. Despite challenges and difficulties encountered along the way, their invaluable assistance and encouragement made this journey possible. During these years, I have also met a lot of good-hearted friends and colleagues who worked hand to hand with me towards achieving this great goal. I would therefore like to pass my sincerest gratitude to them for their support and encouragement. It has been an honor for me to meet and work with such great people.

Finally, I would also like to thank my friends and family out of the University for their support, particularly my parents, my best friend Miss *Gontlemang Leah Letlhoagoje* and my daughter *Resego Latoya Letlhoagoje* for believing in me, and supporting me throughout these difficult years. This piece of work is dedicated to them.

Mr. Lapologang Ntwayame, July, 2017

DEDICATION

This piece of work is dedicated to my Lord Jehovah for making everything that appeared to be impossible before my physical eyes possible – Philippians 4:13 “*I can do all things through Christ who strengthens me*”, to my mother *Miss Kenameditswe Kelebemang*, my grandmother *Miss Pearl Ralekgobo*, my best friend *Miss Gontlemang Leah Letlhoagoje*, together with my daughter *Resego Latoya Letlhoagoje* for their presence in my life.

Table of Contents

DECLARATION AND COPYRIGHT	i
CERTIFICATION.....	ii
ACKNOWLEDGEMENTS	iii
DEDICATION	iv
LIST OF TABLES.....	ix
LIST OF FIGURES	x
LIST OF APPENDICES	xi
LIST OF ABBREVIATIONS	xii
ABSTRACT.....	xiii
CHAPTER 1.....	1
INTRODUCTION	1
1.1 Introduction to the Problem	1
1.2 Background.....	2
1.2.1 Types of Voting Systems	2
1.3 Problem Statement.....	4
1.4 General Objective	4
1.5 Specific Objectives	4
1.6 Research Questions.....	5
1.7 Justification of the Study	5
1.8 Dissertation Structure	6
CHAPTER 2.....	7
LITERATURE REVIEW	7
2.1 Introduction.....	7
2.2 Background.....	8
2.2.1 Countries using E-Voting Systems	8
2.2.2 Barriers and Challenges of Electronic Voting Systems	11
2.3 Security Requirements for Cryptographic Voting Protocols	13
2.3.1 Voter Privacy	14
2.3.2 Eligibility	14
2.3.3 Fairness	14
2.3.4 Uncoercibility	14
2.3.5 Accuracy	15

2.3.6	Individual Verifiability	15
2.3.7	Internet security issues.....	15
2.4	Types of Cryptographic Voting Protocols	16
2.4.1	Non-Cryptographic Protocols	17
2.4.2	Homomorphic Encryption Mechanism.....	17
2.4.3	Mixing Networks Mechanism	18
2.5	General concept of the Envelope Voting Method.....	19
2.6	Cryptographic Digital Signature.....	21
2.6.1	Digital Signature Model/Processes	21
2.6.2	The Importance of a Digital Signature.....	23
2.6.3	Encryption with Digital Signature	24
2.7	Similar Remote Electronic Voting Models.....	26
2.7.1	Framework for an E-Voting System Applicable in Developing Economies	26
2.7.2	Secure Intranet Voting System for Students Union Elections in Nigerian Tertiary Institutions	27
2.7.3	Nigerian Secure Stegano-Cryptographic Voting Model.....	28
2.7.4	A Secure Model for Remote Electronic Voting: A Case of Tanzania	29
2.7.5	Helios Electronic Voting Model	30
2.8	Conclusion on Literature review.....	32
CHAPTER 3.....		34
RESEARCH DESIGN AND METHODOLOGY		34
3.1	Introduction.....	34
3.2	Research Design	34
3.2.1	Descriptive Research Design	35
3.2.2	Quantitative and Qualitative approach.....	35
3.2.3	Methods used to attain Objectives	36
3.3	Research population and sampling	37
3.3.1	Research Population	37
3.3.2	Sampling	38
3.3.3	Sample size	38
3.4	Data collection	38
3.4.1	Questionnaire and interview	38
3.4.2	Secondary Data.....	39
3.5	Questionnaire Design.....	40
3.6	Data processing and Analysis.....	40

3.7	Reliability and Validity.....	40
3.7.1	Reliability	40
3.7.2	Validity	41
3.8	Conclusion	41
CHAPTER 4.....		42
RESULTS ANALYSIS AND INTERPRETATION		42
4.1	Findings from Security and Election Experts (IEC)	42
4.1.1	Description of sample	42
4.1.2	Assessing the current Situation	44
4.1.3	Potential Benefits of introducing an e-voting system in Botswana	45
4.1.4	Potential Challenges of introducing E-voting system.....	47
4.2	Findings from voting populace (voters).....	51
4.2.1	Description of sample	52
4.2.2	Assessing the current situation and problem	53
4.2.3	Potential Benefits of introducing e-voting system in Botswana	56
4.2.4	Potential challenges of introducing E-voting in Botswana.....	58
4.3	Responses from Interviews with security and election experts (IEC)	60
4.4	Cross Analysis of Responses	63
4.5	Conclusion	67
CHAPTER 5.....		68
DISCUSSION.....		68
5.1	Introduction.....	68
5.2	Potential benefits of introducing remote e-voting in Botswana.....	68
5.3	Security challenges hindering introduction of remote e-voting system in Botswana.....	69
5.3.1	Security of IEC ICT Infrastructure	69
5.3.2	Client-Side Attack.....	70
5.3.3	Server-Side Attack.....	71
5.3.4	The Network or Internet Security Attack.....	72
5.3.5	Vote Buying and Voter Coercion	73
5.4	Security Requirements.....	73
5.4.1	Public Key Management.....	74
5.4.2	Identification, Authentication and Authorization Issues.....	75
5.4.3	Addressing Vote Buying and Coercion Problems	77
5.4.4	Ensuring Vote Verification.....	78

5.4.5	Addressing Man-In-The-Middle (MITM) and Denial of Service (Dos) attacks.....	78
5.5	Conceptual Model.....	79
5.5.1	Conceptual Model Architecture.....	80
5.5.2	Conceptual Model Infrastructure	82
5.5.3	Conceptual Model Voting Process.....	86
5.6	Conclusion	88
CHAPTER 6.....		90
CONCLUSION AND RECOMMENDATIONS.....		90
6.1	Introduction.....	90
6.2	Conclusion	90
6.3	Recommendations.....	92
6.4	Limitations	93
6.5	Further Research.....	94
REFERENCES		95
APPENDICES.....		102
Appendix A – Questionnaire Sample for Security and Election Experts		102
Appendix B – Questionnaire Sample for Voting population		105

LIST OF TABLES

TABLE 3.0.1 SUMMARY OF CHARACTERISTICS OF SIMILAR E-VOTING MODELS.....	31
TABLE 4.0.1 - GENDER AND AGE RANGE	42
TABLE 4.0.2 - EDUCATION LEVEL AND WORK EXPERIENCE	43
TABLE 4.0.3 POSITION.....	43
TABLE 4.0.4 - LEVEL OF UNDERSTANDING OF E-VOTING SYSTEM.....	44
TABLE 4.0.5 CURRENT SYSTEM PROBLEMS	44
TABLE 4.0.6 - CAN E-VOTING REDUCE ELECTION PROBLEM IN BOTSWANA?	44
TABLE 4.0.7 - WILLINGNESS TO USE AN E-VOTING SYSTEM	45
TABLE 4.0.8 - VOTER TURNOUT	45
TABLE 4.0.9 - ELIMINATE DELAYS IN BALLOT COUNTING.....	46
TABLE 4.0.10 - PREVENTION OF ELECTION FRAUD	46
TABLE 4.0.11 - SPEEDING-UP THE VOTING PROCESS.....	46
TABLE 4.0.12 –ELIMINATION OF VOTING ERRORS	47
TABLE 4.0.13 - ELIMINATION OF BALLOT COUNTING ERRORS.....	47
TABLE 4.0.14 - IEC STAFF SKILL	48
TABLE 4.0.15 - LACK OF ICT RESOURCES	48
TABLE 4.0.16 - UNSTABLE COMMUNICATION LINK DURING ELECTION PERIOD.....	49
TABLE 4.0.17 - E-VOTING SYSTEM FAILURE DURING ELECTION PERIOD	49
TABLE 4.0.18 - OUTAGE OF ELECTRICITY DURING ELECTION PERIOD	49
TABLE 4.0.19 - SECURITY ISSUES	50
TABLE 4.0.20 - THE COST OF IMPLEMENTING E-VOTING SYSTEM	50
TABLE 4.0.21 - HIGH ILLITERACY RATE	51
TABLE 4.0.22 - WOULD VOTERS BE ABLE TO CONFIRM THEIR VOTES?.....	51
TABLE 4.0.23 E-VOTING USER INTERFACE	51
TABLE 4.0.24 - GENDER AND AGE	52
TABLE 4.0.25 - EDUCATION	52
TABLE 0.26 - PAST PARTICIPATION IN ANY GENERAL ELECTION.....	53
TABLE 4.0.27 - HAVE YOU EVER HEARD OF E-VOTING?.....	53
TABLE 4.0.28 - OPINION ON CURRENT SYSTEM	53
TABLE 4.0.29 - CAN E-VOTING SOLVE ELECTION PROBLEMS IN BOTSWANA?.....	54
TABLE 4.0.30 - E-VOTING INTRODUCTION.....	54
TABLE 4.0.31 - WILLINGNESS TO USE AN E-VOTING SYSTEM	54
TABLE 4.0.32 – RELIANCE ON THE RESULTS OF AN E-VOTING SYSTEM	55
TABLE 4.0.33 - VOTING TECHNOLOGY OF CHOICE.....	55
TABLE 4.0.34 - COMPUTER EXPERIENCE	55
TABLE 4.0.35 - VOTER TURNOUT	56
TABLE 4.0.36 - ELIMINATE DELAYS IN BALLOT COUNTING	56
TABLE 4.0.37 - VOTING FRAUD	57
TABLE 4.0.38 - SPEED-UP VOTING PROCESS	57
TABLE 4.0.39 – ELIMINATION OF VOTING ERRORS	57
TABLE 4.0.40 - ELIMINATE BALLOT COUNTING ERRORS.....	58
TABLE 4.0.41 - IS E-VOTING APPROPRIATE?.....	58
TABLE 4.0.42 - E-VOTING SECURITY ISSUES	59
TABLE 4.0.43 - CAN VOTERS CONFIRM THEIR BALLOT?	59
TABLE 4.0.44 - CORRELATION BETWEEN PAPER-BASED VS. E-VOTING SOLUTIONS.....	64
TABLE 4.0.45 - RELIABILITY AND WILLINGNESS TO USE AN E-VOTING SYSTEM	65
TABLE 5.0.1 DATA ITEMS AND EXPLANATIONS	88

LIST OF FIGURES

FIGURE 2.0.1 THE MIXNET PROCESS USING FOUR (4) NODES [73].....	19
FIGURE 2.0.2 THE DOUBLE ENVELOPE METHOD [21].....	21
FIGURE 2.0.3 CRYPTOGRAPHIC SIGNATURE SCHEME MODEL [56].	22
FIGURE 2.0.4 ENCRYPTION AND DIGITALLY SIGNING USING SENDER’S PRIVATE KEY – SENDER SIDE [56].....	25
FIGURE 2.0.5 VERIFICATION WITH SENDER’S PUBLIC KEY – RECEIVER SIDE.	26
FIGURE 4.1 COMPUTER EXPERIENCE AND TYPE OF VOTING TECHNOLOGY	66
FIGURE 5.0.1 CLIENT-SIDE ATTACK.....	71
FIGURE 5.0.2 SERVER-SIDE ATTACK.....	72
FIGURE 5.0.3 NETWORK-SIDE ATTACK	73
FIGURE 5.0.4 THE DOUBLE ENVELOPE METHOD	76
FIGURE 5.0.5 CONCEPTUAL MODEL ARCHITECTURE	81
FIGURE 5.0.6 CONCEPTUAL MODEL INFRASTRUCTURE COMPONENTS.....	83

LIST OF APPENDICES

Appendix A – Questionnaire Sample for Security and Election Experts

Appendix B – Questionnaire Sample for voting population

LIST OF ABBREVIATIONS

OVS– Online Voting System

DB– Database

E-Voting - Electronic Voting

IEC- Independent Electoral Commission

BIUST- Botswana International University of Science and Technology

ASP- Active Server Pages

SQL- Structured Query Language

HTML - Hypertext Markup Language

MD5 - Message Digest Number 5

SHA-2 (SHA -256) - Secure Hashing Algorithm 2nd Generation

US NIST - United State National Institute of Standards and Technology

ICT - Information and Communication Technology

ABSTRACT

The use of electronic voting systems (EVS's) is seen as an alternative to traditional manual voting because it aims at increasing efficiency, lowering cost of running election, reducing counting mistakes and improving the accuracy of the results. This has led to electronic voting systems being adopted in most countries to replace traditional paper-based voting systems.

Currently, Botswana uses a traditional paper-based voting system. This method of voting comes with several challenges. These challenges include delays in counting of votes and counting errors due to manual counting, a high number of spoilt votes due to wrong markings, and delays in the declaration of election results. These have resulted in voters losing confidence in the current system thus leading to poor voter turnout.

This study therefore explores the feasibility of introducing and implementing of e-voting in Botswana. This study adopted a mixed method to collect and analyze data using purposive sampling technique to consciously select specific respondents, so as to gain insight from them and an in-depth understanding of complex experiences or events. This technique was used to select and administer questionnaires to IEC officers and voters.

The results indicate that respondents have a positive perception towards introduction and implementation of remote e-voting in Botswana. They further indicated that introducing an e-voting system will bring several benefits such as improved voting process, reduced chances of voting fraud, eliminate counting errors, as well as reduce delays in counting and publishing of results. The majority of respondents have indicated that they are willing to use an e-voting system compared to a traditional paper-based voting system. The outcome of this research's findings would form a basis for appropriate recommendation for introduction and implementation of e-voting in Botswana.

Keywords: *RSA signature scheme, Encryption, Decryption, SHA-2 hashing algorithm, conceptual model, e-voting systems, traditional paper-based voting system.*

CHAPTER 1

INTRODUCTION

Elections are one of the key factors that have an impact on the democracy of a nation. Not only do they provide for the orderly transfer of power, but they also cement voter's trust and confidence in their leaders.

Electronic voting technology has been implemented worldwide by different developed countries[1],[2],[3]. The use of such technology helps to accelerate the ballot tallying process and reduce human errors[2], and improve accessibility for disabled and illiterate voters[4]. Therefore, it is important to explore the adoption and implementation of this technology within Botswana. This may help to bring about trust and confidence in using the system, thus boosting future voter turnout.

1.1 Introduction to the Problem

Currently, the Botswana Independent Electoral Commission is still using the traditional paper-based voting system to elect candidates which is found to have major problems. These problems include requirements of extensive electoral staffing, possible misappropriation of ballot boxes, impersonating of voters, and multiple registrations by the same voter may also take place[5],[6],[7],[8]. It also requires accurate hand counting and manual computation of ballots to determine the appropriate winner after an extensive vote verification process[9],[10]. Further to this, an unscrupulous electoral officer can modify results by deliberately mismatching ballots with the candidate they were cast for [5],[7],[8]. This can lead to misaligned voting results leading to non-acceptance of results, violence or even civil war.

Hence there is a need to develop and implement secure models and systems to ensure transparent, accurate, confidential, fair, free and secure processes of electioneering. In this regard, an election system must be robust such that it minimizes fraudulent behavior and for

candidates and voters to accept the results [11]. It is important that election results reflect the true opinions of voters.

1.2 Background

Since the discovery of internet in the early 80's numerous studies on electronic voting have been conducted. Electronic voting systems integrate the use of Information Communication and Technologies to capture, record voter's intention, and display election results[2],[12],[13],[14]. The use of e-voting was adopted to eliminate the cost of generating a paper-based ballot paper[15], it also minimises the cost of transporting physical ballot to different polling stations[4]. Nevertheless, only few governments have made e-voting readily available for use for their citizens [14].

The other means of voting is through the use of paper ballots which are referred to as a traditional voting system[13]. This system uses ballot papers and ballot boxes [2]. This system has a number of advantages because voters still have trust on the system. The other advantage of using this system is that the security is provided by selected candidates are around during voting, normally known as observers. However, these systems are not without problems. Some of these problems include, time-consuming as voting and tallying can take more than a day, whereas in a country with large number of population vote counting and tallying does take longer time to complete. This system is also exposed to fraudulent behavior during elections[16]. To reduce all these problems, remote electronic voting systems have been suggested to allow voters to cast their votes from anywhere in the world and also to speed-up the publication of results[14],[15],[17].

1.2.1 Types of Voting Systems

There are two types of voting systems discussed in this study. These are: paper-based voting system and electronic voting system.

1.2.1.1 Paper-Based Voting System

In this voting system, the voter gets a blank ballot paper from election officials and uses a pen or a marker to indicate their choice. This form of voting was first introduced in Australia, in

1856 [2]. To this day, paper-based voting is still the most common way of voting in most countries[18].

1.2.1.2 Electronic Voting System

a. Stand-Alone Electronic Voting System

Stand-alone electronic voting system involves the use of computers for casting and tallying of votes. There are different types of stand-alone e-voting systems such as lever voting machine, punch card voting machine, direct recording voting machine and optical scan voting machine [14], [11]. These voting systems are classified as stand-alone machines because they are installed in a fixed location such as post offices, shopping complexes or any common location which allow voters to easily access the voting sites. However, these stand-alone voting systems are still inconvenient to voters since it is requisite for the voter to physically present themselves at the voting machine [14]. Voters are not able to cast their votes remotely, on any given platform, without restrictions to weather conditions, location and hardware. These specific traits render the system cumbersome and results in poor voter turnout. Further compounding the drawbacks associated with these voting systems is the high cost of such voting machines [14].

b. Remote Electronic Voting Systems

This type of electronic voting systems also involves the use of computers for casting and tallying of votes. They are not install in a fixed location, which allows voters to cast their votes from any location using devices such as mobile phones and computers connected via the Internet [19],[14]. These systems use modern technologies such as cryptographic and mix net tallying to secure voting systems and ensure confidentiality and trust among voters.

According to studies[8],[19],[20],[21],[22] the foundations of modern cryptographic voting systems were launched in the 1990's by introducing powerful techniques such as homomorphic tallying and mixing networks. These voting systems use a technology known as cryptographic technology. This technology has become an important means of ensuring confidentiality, security, accuracy and integrity in the voting process, notably through the use of encryption key distribution. In 2004, Chaum [7] and Neff [23]proposed acryptographically

secure voting system in which a voter does not have access to the computational device during the voting period.

Encryption is considered to be a mechanism that enables secure communication which includes sending a message from a sender to a receiver over a public channel while keeping it hidden from unauthorized users (eavesdroppers)[19],[24]. In particular, Public Key (RSA) encryption which was first published by Rivest, Shamir and Adleman [25], provides a way for a sender to encrypt a message into a form of ciphertext using the receiver's public key, and for a receiver to be able to decrypt the ciphertext to obtain the message using a private key. The use of this security mechanism gives rise to a number of useful applications in different organizations as they will be able to transmit all their data in an encrypted form and perform computations on encrypted data but only decrypt data when necessary[8],[15],[26]. Cryptographic technology is already useful in a number of applications [6],[8],[27],[5],[28].

1.3 Problem Statement

The problem this research addresses is to design acceptable and satisfactory conceptual voting models detailing what should be included when designing secure remote electronic voting systems which will help to solve the problem of declining voter turnout within Botswana and other developing countries. Therefore, this study proposes a conceptual voting model for designing and implementation of a secure remote electronic voting system for possible adoption within the developing world.

1.4 General Objective

The aim of this study is to develop a conceptual model for designing and implementation of a secure and trusted remote electronic voting system for possible adoption within Botswana.

1.5 Specific Objectives

In order to achieve the main objective of this dissertation, the following specific objectives were derived:

- ✓ To identify the potential benefits of introducing a remote e-voting system in Botswana

- ✓ To identify security challenges from a technical perspective that would hinder the introduction and implementation of a remote electronic voting system in Botswana.
- ✓ To identify security requirements for a remote e-voting system.
- ✓ To develop a conceptual model for designing and implementation of a secure and trusted remote e-voting system for possible adoption within Botswana.

1.6 Research Questions

This dissertation attempts to give answers to these research questions:

- ✓ Can a remote electronic voting system overcome the problem of declining voter turnout?
- ✓ What are the security challenges that would hinder the introduction and implementation of remote electronic voting in Botswana?
- ✓ What are the security requirements for a secure remote electronic voting system?

1.7 Justification of the Study

The main purpose of this study is to develop a conceptual model for designing and implementing of secure and trusted remote electronic voting system emphasizing on security and result's veracity. The conceptual model is aimed at converting the traditional paper-based voting system adopted by the Botswana Independent Electoral Commission. The traditional paper-based voting system is normally held under the supervision of election officials to ensure the right application of electoral rules, that only registered voters cast votes, to curb forgery and attempts of multi-voting. Unfortunately, the process of human supervision over the election process requires a lot of effort, expenses and other resources to achieve the desired levels of privacy, security, accuracy and trust. Despite the best attempts, this system is still beset with human computational errors especially at ballot counting and results tallying. To overcome these problems, electronic voting systems have been developed by different countries and organizations.

This study proposes a conceptual voting model for designing and implementing secure and trusted remote electronic voting systems which will alleviate problems encountered when using traditional paper-based voting systems. The proposed conceptual model uses RSA and

SHA2 algorithms, and mixing net mechanism discussed in details in chapter 2, to ensure the accuracy of the votes and maintain confidentiality by encrypting all the cast votes, voter's information and performs the calculation of the votes during final tallying without revealing any information. This model also aims at providing voter's privacy, safety, verifiability, and correctness.

1.8 Dissertation Structure

This dissertation consists of six (6) chapters. Chapter 1 covers introduction of the problem, background, problem statement, general objective, specific objectives, research questions, justification of the study and dissertation structure.

Chapter 2 gives a detailed background on different types of existing electronic voting systems and models, the importance of strong and secure encryption and hash algorithms in producing secure voting systems with acceptable voting results. It also covers an overview of cryptographic voting protocols (*mix net and homomorphic*).

In Chapter 3, the methods adopted to carry out this research are outlined, and a detailed structure of how this research is going to be conducted is provided, as well as the number and types of targeted respondents, and methods used in selecting respondents.

Analysis of collected data and the results are given in Chapter 4. This chapter covers responses from respondents or security and election experts on how they feel about the developed conceptual model, whether the introduction of e-voting will solve the problem of declining voter turnout or not and also discover challenges hindering implementations of e-voting in Botswana. It also covers the identification of secure requirements for a secure remote e-voting system. Chapter 5 covers the discussion of the findings.

Chapter 6 provides a summary of the dissertation, together with possibilities of future research directions and this is followed by list of materials used when conducting this research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter provides a review of a number of existing cryptographic electronic voting protocols and models focusing on approaches used to design and implement existing voting models and systems based on application requirements. It looks more into cryptographic primitives used in developing existing electronic voting systems and models, examine them and look into how they can be improved. These include re-encryption techniques used for verifying correct shuffling of mixnets and homomorphic encryption schemes[9],[20],[29],[30],[31]. **Homomorphic encryption** can be defined as a form of encryption that allows computations to be carried out on ciphertext without decrypting data first, and this generate correct results from encrypted data corresponding or matching the result of operations performed on the plaintext[31],[32]. A **Mixnet** is a form of cryptographic mechanism which decrypts a set of encrypted messages in such a way that no one will be able to determine the source of the message (plaintext)[33].

Since electronic voting is an area of growing interest[20], a number of researches have been carried out searching for technologies and mechanisms that can be used to bring about trust in electronic voting systems to users[21]. Therefore, this chapter looks at the descriptions of modern techniques and solutions which can be used to solve the problems encountered when using traditional paper-based voting systems. It also looks at requirements, challenges and security issues of these methods, and reveals the main differences in security property classes. It also creates space for future selection and design of secure and accurate online voting systems as well as theories related to cryptographic digital signature schemes used in modern voting system solutions.

2.2 Background

Based on the existing literature, there are various cryptographic schemes developed and implemented worldwide, by different depositories with a goal of achieving accuracy, security and transparency in the voting process [34],[35]. Some of these schemes are homomorphic encryption, blind signature, and mixnets [4],[36],[37].

Homomorphic encryptions were first introduced by Josh [32] and Benaloh [24]. This scheme establishes universal verifiability in the election systems by simply generating a new encrypted vote as the product of the two votes. The product of the ciphertext of any given two votes is the ciphertext of the “sum” of the votes. The reason behind the homomorphic encryption is that ciphertext of the sum of the ciphertexts of the votes can be decrypted from each encrypted vote into the original format. Homomorphic encryption was further improved by [38]. Since then, a number of improved schemes have been developed by different depositories [17],[39]. The **blind signature schemes** were first introduced by Fujioka *et al* [4],[36],[37]. These schemes are derived from digital signature and they have some additional features. A blind signature is a protocol that is used to obtain a signature x on y from the signer S in such a way that S does not learn anything about x and y [40]. These schemes were further improved by Chaum [41].

Schemes based on **mixnets** have been developed along with the mixnets in order to provide voter privacy in voting schemes [42]. A simple way to achieve voter’s privacy when using mixnet schemes is to shuffle the number of votes from different voters using **mixnets** [42]. A mixnet shuffles its input in a way that no element of the output can be linked back to any element in the input. To ensure that the link between the input list and the output list is not retrieved, the mixnet alters the appearance of each message without affecting the original meaning of any message in order to maintain accuracy [43]. The **mixnets** approach is also used in onion routing [44], which provide anonymous routing.

2.2.1 Countries using E-Voting Systems

The design, development, and implementation of secure electronic voting systems have been adopted by different countries to carry out general elections [13]. Countries adopted e-voting

systems are discussed in this chapter. This helped the researcher to understand the current state of e-voting systems and challenges faced during adoption and administration of these systems. These countries are Estonia, Venezuela, India, and United States of America.

2.2.1.1 Estonia

According to [13],[45], Estonia introduced remote electronic voting as an additional voting channel for general elections in 2005 and enjoyed widespread trust from the beginning. Estonia is modern country which heavily relies on the Internet. Most of the things in Estonia are done through the Internet linked to citizen's electronic national ID (eID). These cards are also used during the election when using the e-voting system [46]. Estonian still maintains and uses the e-voting system for the parliamentary elections since 2005 [47], [48].

ID Cards and PKI (Public Key Infrastructure): The ID cards are built on a Java chip platform, which contains a 2048-BIT PIN protected with RSA key-pair and creating signatures with SHA1/SHA2 [40], [26]. This conforms to common security practices in the Web and can easily be used for authentication, encryption and signature. Since the government distributes the ID cards, they keep track of the public keys used by the citizens. Therefore, authenticating at the electronic voting system and validating the eligibility is easy, because the voter just has to create her signature with the ID card, send this signature to the application's authentication servers and is authenticated through the government's PKI.

Therefore, this study adopts this remote electronic voting model used by Estonia because the concept of public key cryptography is well understood and it is generally easy to implement. Therefore, explaining the concept to voters becomes much easier and there are several libraries existing to be used in the source code of the voting system.

2.2.1.2 Venezuela

Since the introduction of Direct Recording Electronic(DRE) voting system in Venezuela in 2004, trust in the impartiality of e-voting was very low and voters did not have trust in using the system as they believed it would be used to manipulate voting results [45]. This system also had technical weaknessessince it neither minimized nor eliminated the possibilities of

cross-checking votes and voter's information. It therefore created a critical situation a few days before the 2005 election whereby residents and stakeholders refused to use the system due to lack of trust[45].

To restore credibility, the effective measure included massive paper trail recounts in 45% of the polling stations, which was far more than the small statistical samples that are normally accepted as sufficient as well as the elimination of the automated identification process[45]. This rendered the voting process very expensive and no longer costeffective compared to traditional paper-based solutions. The traditional paper-based voting method was found to be the only way to remedy the lack of trust voters had on using the technology-based method.

2.2.1.3 *India*

India introduced the use of electronic voting since 2002[45]. The voting machines adopted in India are considered to be the cheapest and use relatively simple technology[45] among all the countries using voting machines. The Indian system has no paper trail option which is highly recommended for fair elections in any country using electronic voting systems. However, the simplicity and insecurity of the system created disagreement among voters as they were saying the system contains security problems. This led to the Indian International Electoral Committee (IIEC) to consider the introduction of the paper-based voting in 2010[45].

2.2.1.4 *Norwegian –I-Voting System*

Norway started using remote electronic voting system to conduct general elections in 2011 [21]. The general design of Norwegian I-vote system is more similar to the Estonian voting system, but it has other decisions regarding the design, which will be explained in this subsection. Norwegian i-voting system was presented as the first governmental voting system fulfilling the requirements for coercion-resistance and voter verifiability.

Many institutions on Norway rely on MinID, which “*provides access to public services at a medium-high level of security*” [50]. Therefore, the maintainers also rely on this service, because it provides a secure authentication mechanism and is already accepted by the Norwegian citizens. It is free of charge and can be used to login to the e-voting system with the voter's national identity number, password and PIN code.

The e-voting client is written in Java and contains the election's public key like the Estonian voting system and encrypt ballots using public key. A signature is added with *MinID* and this double-envelope ballot is sent to the ballot box. Norway implements its voter verification functions in a different way as compared to the Estonian voting system. Here, the voter gets a poll card via postal mail containing a list of all parties and a corresponding four-digit code individually calculated for each voter. After the voter placed her ballot, the voting server sends an SMS to the voter's mobile phone containing her own 4-digit code. Now the voter can compare if the code received matches the code of the chosen party on the roll card. This gives the voter the possibility to verify the cast vote.

To rectify coercion problem, Norwegian voting system allows voters to vote more than once, and only the last vote will be counted and the previous votes are automatically rejected.

This process of voting takes long to compute the results, therefore this system may not be applicable to countries like Botswana because it is not everyone having a postal address (Postal Box) hence this will limit them from participating during elections. Therefore, to improve this voting model process, the proposed model uses a different tallying process from the Norwegian voting model by adopting homomorphic encryption. The proposed voting model compresses the encrypted votes and then exponentially combines the ciphertexts. This might significantly reduce the computational time and make it more suitable for tallying the ballots.

This study adopted this model process of voting to improve voter verification process through the use of cryptographic security. Norwegian voting model also uses double envelopes as well as mixing net to achieve a reliable anonymity of the ballots. This model allows return-codes which gives voters the possibility to verify their votes. These are important steps towards a secure and verifiable voting system, though it needs some improvement in operational security, universal verifiability and the development model.

2.2.2 Barriers and Challenges of Electronic Voting Systems

This sub-section covers barriers and challenges encountered when adopting and using the electronic voting system. The developed conceptual model allows for the reuse of

important concepts and results proven for the broader setting, hence fulfilling some of the crucial security requirements which may lead to success or failure of the voting system if not implemented properly[30],[43],[35],[51].

This sub-section introduces both general and votingspecific definitions that will help in the understanding of the specific challenges of electronic voting. It introduces and defines the notions of accuracy, privacy, software independence and end-to-end security.

2.2.2.1 Software and Hardware Reliability

Machine failure is one of the concerns when it comes to using e-voting systems [27], [33], [52]for example, if there is a power outage during voting, this may leave votes uncounted or miscounted without any means of recovery [4], [53]. Poor system design can lead to the developed system being complicated and complex to operate[15],[29], [33]. Some of the systems are intended for operation without obvious protective measures and deployed without thorough and scientifically designed testing plans [38], [54]. Additionally, machines may prevent people from voting if the system itself becomes overloaded with voter's requests to vote, and may crash or freeze causing delays in voting [55].

2.2.2.2 Hacking

Using electronic voting systems brings with it challenges which include hackers. They can successfully hack into an electronic voting system and steal votes using malicious programming approaches, corrupting data and altering votes by either adding or removing votes[4],[31],[56]. A system can also be susceptible to spoofing and “man in the middle” attacks from hackers[4].

2.2.2.3 Accuracy in capturing voter's intent

When dealing with electronic voting machines, there is a possibility of misaligned voting where a voter castsfar more or far less votes than the required number[4],[14]. Touch-screen machines can also misinterpret a voter's intent[24]. For example, a voter might touch the part of the screen identified with his preferred candidate *Joseph*, but candidate *Adam*'s box would light up instead hence leaving a voter with no choice but to choose anunintended candidate.

2.2.2.4 *Attachments from malicious software*

In as much as computers are involved in the casting process, they are particularly prone to attacks from malicious software such as viruses and worms that are programmable to manipulate votes in favor of certain candidates while maintaining appearances of normality[18].

2.2.2.5 *Domain Name service attack*

When using the Internet to cast votes, there is always a possibility of Denial-of-Service attack (DoS)[7],[26],[56]. This attack when using the network or the Internet for voting, it exposes the election process to a higher risk or degree of disruption by outsiders or intruders [26], [58]. This kind of attack was reported to have taken place during leadership convention in the Canada (Toronto) in 2001, which caused a delay in voting [18].

2.3 Security Requirements for Cryptographic Voting Protocols

Remote electronic voting in most cases takes place over the Internet[5],[11],[15] which is an environment that is not transparent and it cannot be easily monitored by electoral officials and is accessible on a global scale[9],[31]. It can therefore be tampered with on a wider scale than traditional types of voting[31]. As such, security and accuracy are critical factors if voters are to cast their votes via the Internet[4].

In order for a remote e-voting system to be considered trustworthy, it needs to meet certain security requirements[36]. Security can be defined in many ways within the context of voting, whether it is in traditional or remote electronic voting[9]. Security can refer to the technical aspects of ensuring respect to confidentiality, integrity, trustworthiness and availability in voting[9]. It can also be referred to as a whole range of functions and components of elections, such as registration, eligibility, verification and authentication[59].

The remote e-voting system should be protected against accidental or intentional denials of services[14]. It should also be availed to all voters whenever the service it offers is needed. The unavailability of the voting system (or one of its components) may result in the loss of a voter's capability to exercise their fundamental political rights of voting [13].

2.3.1 Voter Privacy

Voter privacy must be preserved throughout the election process in such a way that no one should be able to trace any relationship between registered identity, the voter's public keys, and cast votes[17],[55]. Moreover, no one should be able to trace the IP address of the voter to establish the relationship between the voter and his vote. According to literature, privacy is one of the critical factors that leads to poor voter turnout in most cases[4],[7],[43],[55].

2.3.2 Eligibility

The system should only allow eligible voters to cast votes[14]. Registration of voters before elections is done to ensure that all voters who qualify to partake in elections are registered before elections. During registration, it is rigorously ensured that only true citizens of that particular country, being of legal age and bearing valid identification credentials are registered to ensure that the “*one-voter one-vote*” law is applied across the board[19]. Registration and authentication in voting systems are normally used as procedures to ensure that only registered and eligible voters are permitted to cast votes and also to ensure that elections are not rigged[13],[14].

2.3.3 Fairness

There should be no partial tally revealed to the voters, candidates or even the International Electoral Commission Officer (IEC) before the end of the election period to ensure that all the candidates are given a fair decision[14]. When using electronic election, the system should be transparent to both voters and candidates, and no one should be able to manipulate the election results[4]. This can be brought about by including the participation of several entities with each assigned specific duties or tasks[13] in the system's critical operations.

2.3.4 Uncoercibility

Coercibility is common in developing countries, due to poverty and a high number of unemployment most especially among the youth[14],[35]. According to literature, for an election to be free and fair, it has to be conducted without any violence, coercion, pressure,

manipulative interference and other influence, practiced by the state or advantaged candidates[5],[9],[29],[60],[61]. Therefore, coercion by either authorities or an agent of the state should not be able to change the value of the voter's choice to cast their vote in a particular way[20]. To prevent or reduce the existence of vote buying and coercion, voting systems need to be designed and developed in a way that no voter will be able to prove that he voted in a particular way (traceability on the part of the voter)[31].

2.3.5 Accuracy

An accurate system should ensure that the outcome of election results corresponds to and depicts what voters voted for[4]. The ballot that is transferred to the votes counting server should be in an accurate state, not a modified copy of the voter's choice[21],[58]. Additionally, the voting system has to be sufficiently robust to exclude a non-valid vote from tabulation and include all valid votes in the final tabulation[62].

2.3.6 Individual Verifiability

This indicates that each registered voter can verify that his vote has been counted correctly in the final tally by just using published data[4]. A trustable electronic voting system should allow for verifiability, both by voters, election officials, all contesting parties and independent election observers[13]. This brings transparency and boosts trust which may lead to improved voter turnout.

2.3.7 Internet security issues

Voting over the Internet is exposed to potential risks due to the insecurity of both the machines used by voters and the network connection which connects the voting machines to the voting server[8],[13],[63]. Despite the widespread use of anti-virus software and firewalls used to protect the voting machines and applications[4],[7], the voting machines used by voters may be infected with different types of computer viruses, Trojan horses, worms, and spyware applications which may be programmed to manipulate their contents[13],[15],[30].

The introduction of cryptographic voting protocols helps to reduce the potential risks of casting votes online and also allows a degree of confidence in using this mode of voting due to the security and accuracy base provided[19],[24].

In addition, the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols were introduced in voting processes to prevent attacks such “*man-in-the-middle*”[20]. This attack refers to a situation whereby an attacker hijacks a network transmission and controls the channel through the two endpoints of the transaction that communicate with one another[55]. The other attack associated with Internet security is known as denial of services (DoS). The attacker normally interrupts communication between the voter application and network server or between the network server and Back-Office (server side)[15] by overloading one of the communication endpoints[64]. The other attack known as spoofing[4], refers to a situation whereby one of the communicating parties is tricked into opening an insecure link controlled by the hackers. This attack can use an email and send it to a voter containing a masked link to a particular site, which has been created to perfectly fake the targeted website together with a request for a voter to “re-enter” his personal information such as username and password or credit card number etc.[12],[26],[65].

When using the Internet to carry out elections, security has to be guaranteed in order to boost voter’s confidentiality and trust in using remote electronic voting systems, hence increasing voter’s turnouts which are the main concern of this research.

2.4 Types of Cryptographic Voting Protocols

According to literature, cryptographic voting protocol has its origin from over two decades of cryptographic research[9],[12],[15],[22],[29]. The use of cryptographic protocols in voting was first brought into use by Chaum in 1981[33],[42]. The introduction of cryptography in electronic voting systems was mainly to improve system security and privacy which can lead to voters gaining confidence in using this method of voting hence improving voter’s turnout[33].

These protocols focus on voting over the Internet with trusted desktop machines, and other electronic voting methods using End-2-End(E2E) schemes where voters cast their ballots

through a paper-based method or obtain a paper receipt from a polling site[12],[20] e.g. DRE machines.

There are three main protocols used for creating cryptographic voting systems and models, and these are *non-cryptographic protocols*, *homomorphic encryption protocol*, and *mixing network protocol*[9],[19],[29]. The following subsections give a detailed description of each.

2.4.1 Non-Cryptographic Protocols

According to literature, there are four existing proposals using this method, *Farnell*, *ThreeBallot*, *Vote-AntiVote-Vote* (VAV), and *Twin*[30],[66]. Each of these proposals allows the voter to hide in the noise of the system while providing a checkable receipt[66].

The two protocols using “Floating receipt” include, *Farnell*[30],[66] and *Twin*[67]. The voter can vote as normal with a paper ballot containing a serial number for verification. When a voter casts their ballot, they receive a copy of a randomly selected previously cast ballot. Therefore, if all the voters can verify their ballot receipt and we can trust the random selection process, there will be a high probability that any change made will be easily detected[30]. Farnell is slightly more complex than Twin because it does not have any take-home receipts. Instead, the voter signs a ballot and casts it into a second ballot box[67].

The ThreeBallot and VAV [68],[69] uses multiple cast ballots to allow voters to hide in the noise. Both systems allow voters to fill out each of the multiple ballots, all machines used are trusted to check whether all the ballots are filled out correctly, and after voting, the voter takes home one of the ballots as a receipt.

2.4.2 Homomorphic Encryption Mechanism

Homomorphic encryption is a cryptographic system that permits the ciphertext (encrypted plaintext) to be added together to produce a summation that, when decrypted, produces a sum of the plaintext[40]. A typical example, suppose we have an encryption function E , decryption function D , key k , and a set of numerical plaintext p_1, p_2 , then[8],[70]:

$$D_k(E_k(p_1 + p_2)) = D_k(E_k(p_1) + E_k(p_2))$$

It is not always the case that the ciphertext will be the same for both encryptions, only the decryption function has to produce the same results matching the encrypted plaintext. According to [71] and [26], homomorphic systems are the same as public-key systems, as they both provide an advantage as generating the ciphertext can be done by a third party without giving them information that might decrypt another ciphertext. Examples of systems using homomorphic cryptology are; *ElGamal*[40],[56], *Paillier*[72] and *RSA*[25].

ElGamal encryption uses multiplicative homomorphism[40]. So if the encryption of the message $m1$ and the encryption of another message $m2$ is multiplied together, the results will be the encryption of the product[40]. So what happens with ElGamal is that when two encrypted messages are multiplied together, the randomization gets added up together in the exponent and the messages get multiplied as well[19]. The snipped code below shows how encryption is computed when using ElGamal encryption algorithm[19],[40].

$$E(m1) * E(m2) = E(m1 * m2)$$

With RSA, the operation is different though both are homomorphic cryptosystems. When using RSA, after encrypting a plaintext P into ciphertext C , multiplying C with 2 and then decrypt $2C$, it gives $2P$ as the output[25]. This will not be possible when using a normal symmetric cipher (DES, AES) because when multiplying an AES ciphertext with 2 and then decrypt it, it will not give P as the case with RSA[25], but some random wrong outcomes.

2.4.3 Mixing Networks Mechanism

According to[33],[42],[58],[73] mixing network mechanism was first introduced by Chaum. A mixnet decrypts a set of messages in such a way that no one will be able to recognize the source of the message[40]. This technique is now commonly used in today's electronic voting systems to bring about security, trustworthiness, accuracy, and privacy in the voting process[73]. This is similar to voting whereby paper slips are placed into a box and shaken, effectively mixing the ballots so that no one will be able to trace back the ballot to its voter rendering traceability impossible[58]. Using this technique in voting systems will help observers to verify that messages were not added, deleted, or even modified by the system or intruders[58].

A mixnets comprises of a series of nodes that partially decrypts input messages and applies a random permutation to the order of the messages it receives before sending them to the next nodes within the mixnets[42]. In order to create anew message, the sender uses the public key p , of each node and then encrypts the message in a reverse order[31],[33]. For example, when using a mixnet of four (4) nodes as displayed in **figure 2.0.1**, the mixnet encryption, ME , of each message, m , would then be[31],[33]:

$$ME(m) = E_{p1}(E_{p2}(E_{p3}(E_{p4}(m))))$$

The mixnet performs the decryption process by using the private key, k , of each involved node as below[31],[33]:

$$m = D_{k1}(D_{k2}(D_{k3}(D_{k4}(ME(m)))))$$

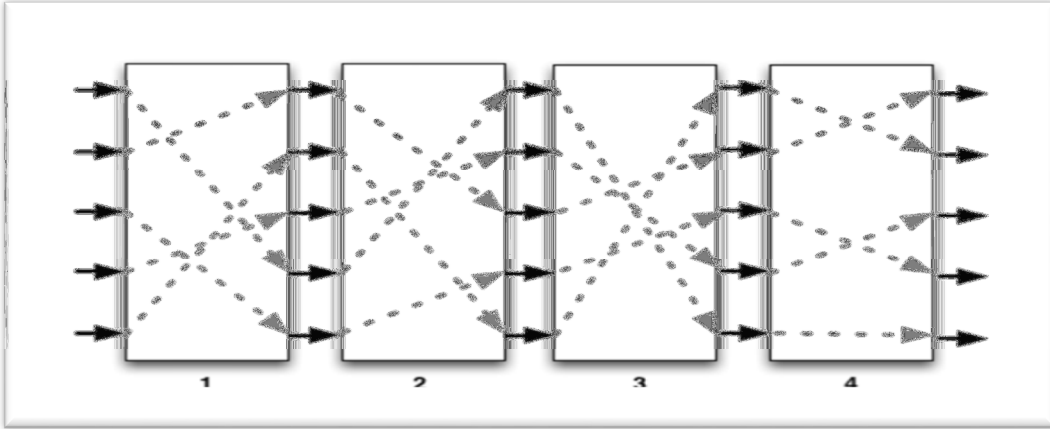


Figure 2.0.1 The Mixnet process using four (4) nodes[73].

2.5 General concept of the Envelope Voting Method

The concept used for cryptographic electronic voting systems is much similar to the envelope voting method. This method is normally used for voters who are abroad or outside the country to cast their votes. The process of voting is given below:

- ✓ The voter identifies himself to the election commissioners
- ✓ The voter selects the candidate of choice by marking the ballot and places it into an inner envelope.

- ✓ That envelope is placed into another envelope in which the voter's details are written on.
- ✓ The envelope is then routed to the voter's polling station via the post office.
- ✓ Upon arrival, the voter is notified that his vote has been received, and the voter's eligibility is verified, and if the voter is found to be eligible, the outer envelope will be opened and then the anonymous inner envelope will be placed into the ballot box and then combined with the rest of the ballots.

The figure 2.0.2 illustrates the Envelope voting method

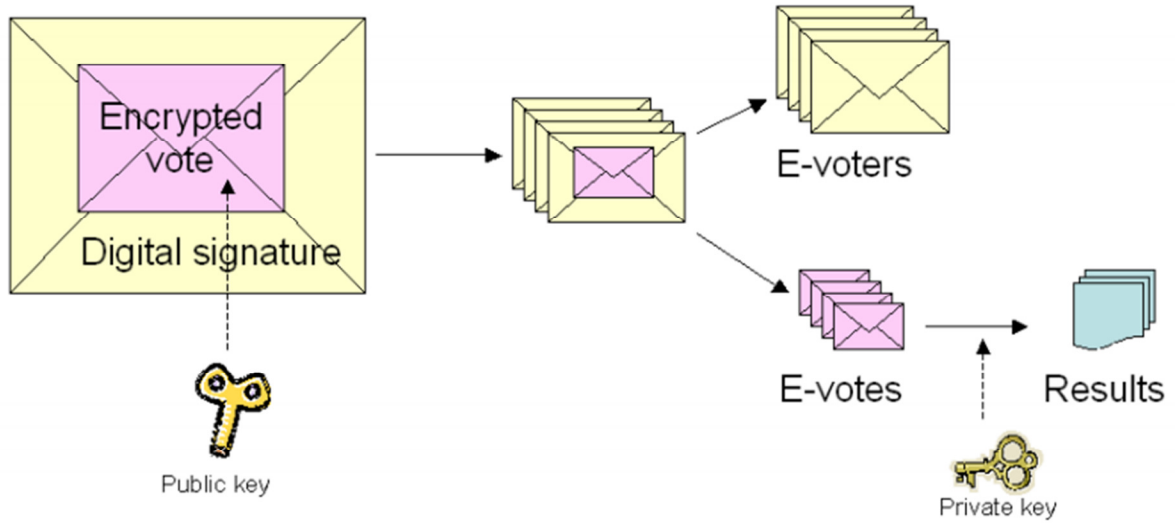


Figure 2.0.2 The Double Envelope Method[21].

Cryptographic e-voting methods follow the same scheme to improve security, privacy, and accuracy within the voting process[21]. When using the e-voting method, the voter's ballot is encrypted using the receiver's public key (Votes Counting Server) and signed using the voter's private key to produce signatures.

2.6 Cryptographic Digital Signature

Digital signatures can be defined as the public-key primitives of message authentication[74]. In the physical world, we normally use handwritten signatures to uniquely verify our identity on typed messages (e.g. application letters), legal proceedings or transactions. Normally digital signatures are used to bind the signatory to the message by uniquely identifying the originator of the digitally signed data and also ensures that there is no tampering or corruption of the signed data[74].

2.6.1 Digital Signature Model/Processes

As explained by literature the digital signature scheme is based on public-key cryptography[9]. The **figure 2.0.3** illustrates the cryptographic signature scheme model.

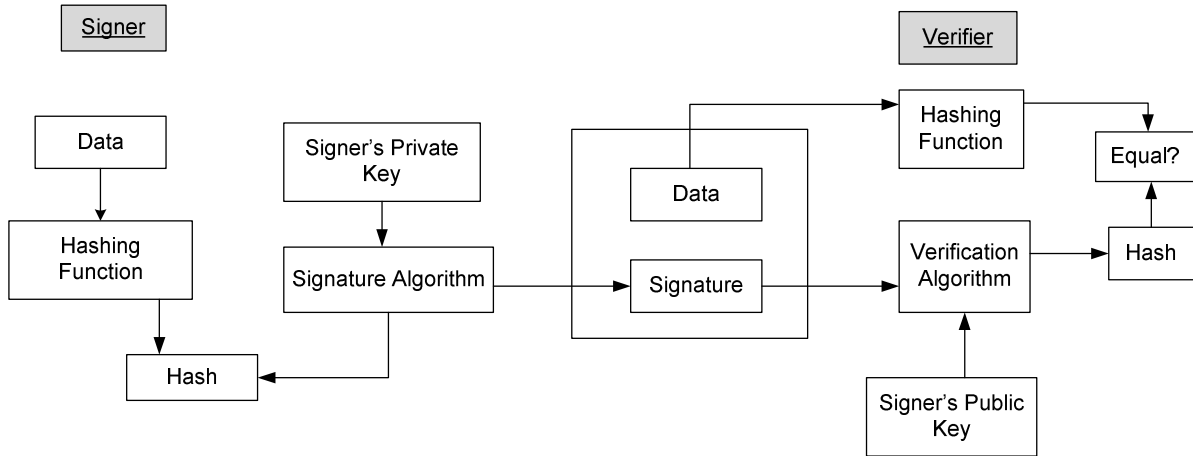


Figure 2.0.3 Cryptographic Signature Scheme Model [56].

- ❖ Each person adopting cryptographic signature scheme should have two cryptographic keys (public-private key).
- ❖ Generally, the key pairs used for encryption and decryption are different from the key pairs used for signing and verifying of data. Normally the private key $SK[i]$ used for signing is referred to as the signature key, while verification is undertaken with voter's public key $PK[i]$.
- ❖ The signatory feeds data to the hash function and generates a hash of data.
- ❖ The hash value and signature key are then fed to the signature algorithm which is responsible for generating the digital signature on a given hash. The signature is affixed to the data before both of them are sent to the Vote Verification Server (VVS).
- ❖ Then Votes Verification Server feeds the combination of the digital signature and the verification key into the verification algorithm. The verification algorithm will then give out some values as output.
- ❖ The verifier on the server side runs its own hash function to generate a hash value which will be used for verification purpose.
- ❖ During verification, the generated hash value and output of verification algorithm are compared. The decision whether modification took place or not is made based on the comparison result.
- ❖ This gives us an assurance that the voter cannot repudiate signing the ballot in future because the digital signature is generated by the voter's unique private key and no one else can have that particular key.

When adapting this model for securing remote electronic voting systems, it should be noticed that instead of signing data directly by signing algorithms, a hash of data (message digest) is created by using hash functions[74]. Since the hash of data is a unique and irreversible representation of data, it is sufficient to sign the hash in place of data. And the most important reason of using ahash instead of data directly for signing brings about efficiency and accuracy of the scheme.

For the developed systematic voting approach,the RSA digital signature scheme was adopted which despite being very slow is more secure. As discussed in *sub-section 2.6.2*, the encryption/signing process using RSA involves a slow and time consuming, but more secure[56]modular exponentiation[19],[22]. Cryptographic schemes differ in terms of performance and security;Schemes which are fast, tend to be less secure and schemes which are slow are very secure[56]. Since the proposed research aims at producing a cryptographic model which can be used for developing secure and accurate voting systems, the RSA digital signature was chosen due to its security factors. When hashing data to produce a message digest (hash) it produces arelatively small digest of the data, hence signing the hash becomes more efficient than signing the entire data.

2.6.2 The Importance of a Digital Signature

According to the reviewed literature, of all cryptographic primitives, the Digital Signature using public key cryptography is considered to be a very useful and important tool to achieve information security [9],[19],[74]. Besides the ability to provide non-repudiation of themessage by the digital signatory, it can also provide message authentication and data accuracy at the same time[74]. The following description gives clear details on how this can be achieved by using a signature.

- ✓ **Message Authentication** –brings about assurance because when the verifier uses the senders' public key to validate the digital signature he is assured that the voter who created the supplied signature is the owner of the corresponding secret private key $SK[i]$ not anyone else[19],[74].
- ✓ **Data Accuracy** – incase when an attacker has access to the data and modifies it, the digital signature verification at the receiver side will detectthe change and notify the

sender that the message has been modified. This is because, when data is modified during transmission, the hash value of the modified data will not match with the output provided by the verification algorithm[20]. Therefore, the receiver can safely deny the message assuming that data integrity has been breached. Ultimately, the breached encrypted vote will be cast to a rejected list rather than sending it to the voting server (database) to wait for tallying and give inaccurate results[19].

- ✓ **Non-repudiation** – when using this scheme, it is assumed that only the signatory has the knowledge of the signature key, so only he can create a unique signature on given data[4],[26]. Therefore, whenever a voter or a third party does not agree with the results, the verifier can simply present data and the digital signature to that particular party as evidence [4]. Furthermore, when a voter wants to confirm that their vote has been *recorded-as-cast* or *tallied-as-recorded* the IEC officers can easily provide the evidence to the concerned voter.

Basically by adding public-key encryption to the digital signature scheme, one can create a cryptosystem that can provide the four essential elements of security namely: Privacy, authentication, accuracy, and non-repudiation. The digital signature scheme was adopted to produce digital signatures in order to meet the aim of developing a cryptographic model which can be used for designing and implementing secure and accurate remote electronic voting systems.

2.6.3 Encryption with Digital Signature

Literature shows that in many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality[9],[43],[74],[75]. In a public key encryption scheme, a public (encryption) key of a sender is made readily available in the open domain, and hence anyone can spoof his identity and send an encrypted message to the receiver. Therefore, making a digital signature technique is essential for users to easily employ public key encryption when encrypting their data, and this will bring about assurance of message authentication and non-repudiation[19],[74].

To achieve this, the digital signature needs to be combined with an encryption scheme. With the developed model, RSA digital signature scheme is combined with the RSA encryption

algorithm and SHA-2 hashing algorithm. When performing this concept, there are two possibilities being *sign-then-encrypt* and *encrypt-then-sign*. However, literature proves that a cryptosystem based on *sign-then-encrypt* can be easily exploited by hackers who spoof the identity of the sender and thereafter changes the message content[9],[15],[29],[30]. Hence, the method is not recommended for use, more especially when measuring security as the proposed research does. **Figure 2.0.4** illustrates how this works.

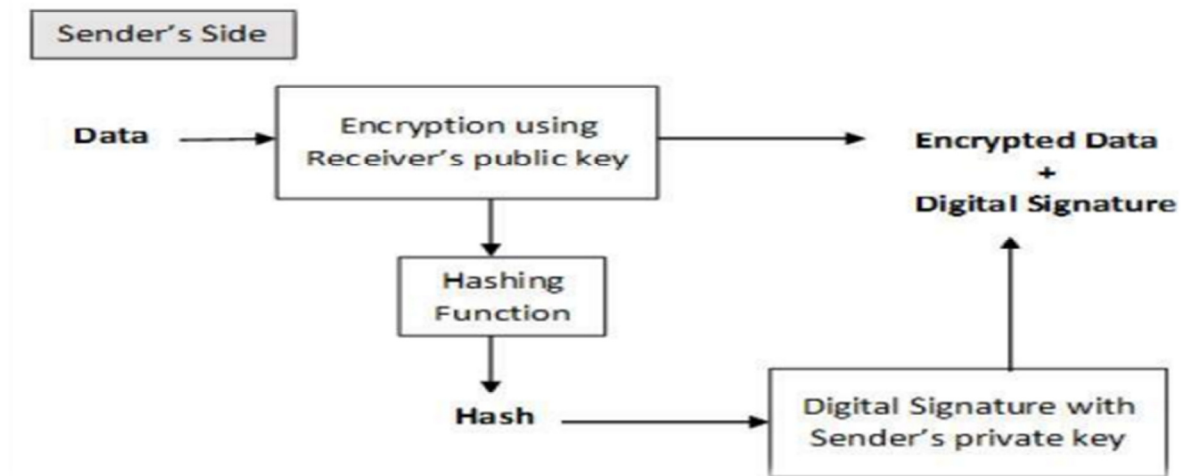


Figure 2.0.4 Encryption and Digitally Signing using sender's Private Key – Sender Side[56]

At the receiver side, after receiving the encrypted data together with the signature on it, the receiver will then verify the signature using the sender's public key $PK[i]$. After verifying the signature of the sender, he can now retrieve the encrypted data by using his own private key to decrypt the ciphertext. The **figure 2.0.5** demonstrates the process.

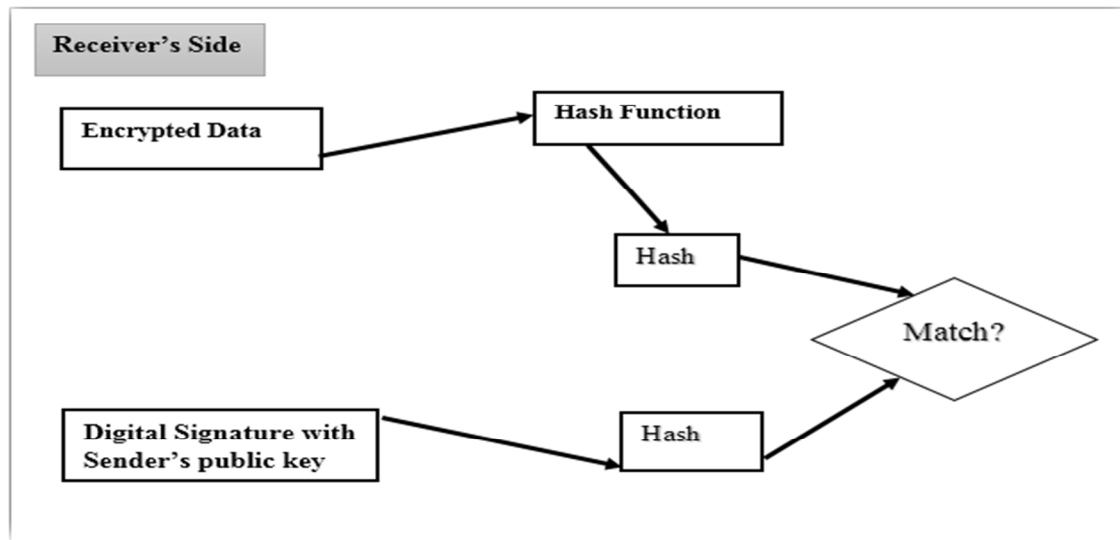


Figure 2.0.5 Verification with Sender's Public Key – Receiver Side.

2.7 Similar Remote Electronic Voting Models

2.7.1 Framework for an E-Voting System Applicable in Developing Economies

Muhammad and Oluwafeni[76], proposed a conceptual framework for an electronic voting system that can be adopted for use in developing economies. The aim of this system is to ensure the availability of the system to only eligible voters and integrity of the voting process through its capacity to identify and prevent ineligible voters and multiple voting. The framework supports both offline and online voting capabilities to guarantee accessibility to all eligible voters to ensure a free and fair election.

Just like the proposed model, this framework[76], ensures that the components of security focuses on the capacity of the system to identify and prevent ineligible voters and multiple voting, thereby ensuring only eligible voters do cast their votes.

The proposed framework [76], combines the capabilities of the Direct Recording Electronic (DRE) and online voting system, offering a platform for online and offline voting. This framework supports voting through direct-recording, online poll-site, and remote voting, which gives voters a platform to choose voting method of their choice. To support online voting, it is implemented as a cloud application. This involves the use of Platform as a Service

(PaaS) arrangement, where operating system, servers, network, memory and other hardware resources are provided by the cloud service provider. Voting is done online either by remotely through a PC connected to the Internet, or at an e-voting polling kiosk. The Direct Recording Electronic machines are administered at a polling kiosk implemented with a computer connected to a keyboard or touch screen for voters to cast their votes. The cast votes are stored on a computer local memory, and the final results will be synchronized with the cloud.

This kind of systems cannot be adopted in countries like Botswana due to the cost of running and acquiring such equipment. Further, these systems are susceptible to exploitation by malicious voters.

2.7.2 Secure Intranet Voting System for Students Union Elections in Nigerian Tertiary Institutions

Molokwu and Agu [77], proposed a model for the design, development and implementation of a Secure Intranet Voting System (SIVS) for Student Union elections in Nigerian Tertiary Education. The proposed system model harnesses and utilizes the immense power of ICT technologies to create a striking impact in the way electoral activities are been conducted in Nigerian institutions. The goal of the system is tailored at establishing an efficient and effective electronic voting system aimed at improving student's democracy, and reducing electoral irregularities and malpractices in student's union elections through a combination of robust voting technologies.

This system model is divided into different phases, the first phase comprises of System Identification (SI). The Identification System aids in unique identification of student or user of the voting system. Thus the system depends on the database of student's academic profile for user identification. During this process of user identification, an eligibility check is performed based on the student's database profile. The second phase covers the ballot being transmitted to the Voting System, which then executes an integrity check on the ballot. Afterwards, the vote will be made anonymous through the use of homomorphic encryption mechanism. Thirdly, the cast ballot is transmitted to the Counting System. Here, there are two established methods that can either be used to accomplish this transfer, being (a) *With a physical medium through an air-gap, or (b) by internal network connection.*

The Counting System mixes the ballots or votes before encryption and counting in order to guarantee a high level of anonymization and security. The last step is the Publishing System which covers publication of the results via the Intranet or within a Local Area Network.

This system model is only suitable and accommodated for the coverage of a small group of people such as schools and tertiary institutions. The architecture adopted would not fulfill all the security requirements standards set for general election e-voting systems. The voting process would not be secure since local voting station and central Database (DB) server were placed on the same local network and encryption schemes adopted were also not discussed.

2.7.3 Nigerian Secure Stegano-Cryptographic Voting Model

Olaniyi *et al.* [75], proposed an enhanced stegano-cryptographic model for secure electronic voting system in poll-site, web and mobile voting scenario for better citizen's participation and credible e-democratic election. The electronic ballots are encrypted using Elliptic Curve Cryptography and Rivest-Shamir-Adleman (RSA) cryptographic algorithm. The encrypted ballots are scattered and hidden in the Least Significant BIT (LSB) of the cover media using information hiding attribute of modified LSB-Wavelet steganographic algorithm. The image quality of the model, stego object was quantitatively assessed using Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Root Mean Square Error (RMSE) and Structural Similarity Index Metrics (SSIM). This system aims at providing eligible voters with a means of exercising their right to vote through the use of a remote voting system using electronic devices at their own pace and time without visiting polling stations. The system aims at increasing participation, confidence and trustworthiness in electronic voting systems [75]. However, the description of the system itself is very inconsistent and confusing as they are existing descriptions about the encryption of the ballots which are simple and easy to understand. Once more, it is not possible to peer-view the code [9], [41]. This is not a good practice, because only few people with access to the source code are able to check it for bugs or malicious code. Creating an open source voting system is essential for a system that shall be trusted during an election. The system model [75], also doesn't cover coercion-protection as voter only needs some credentials and is able to vote. Therefore, vote-selling and coercion are a big issue and should not be underestimated.

With the proposed model, to avoid vote selling or coercion, votes are allowed to vote more than once and only the last vote will be counted. So in this case, the coercer will never be sure which vote was tallied. The voting system also focuses on voter verifiability and besides the cryptographic mechanism adopted, the system uses double envelop method in **sub-section 2.5**, the mixing achieves a reliable anonymity of the ballots and the return-codes give the voter the possibility to verify her vote. These are important steps towards a secure and verifiable voting system.

2.7.4 A Secure Model for Remote Electronic Voting: A Case of Tanzania

The author of [78] presented a secure model for implementing of remote electronic voting through the use of mobile phones or Internet to be used for future presidential and parliamentary elections in Tanzania. Authors reviewed several remote electronic voting models, analyzes them and identified their strengths and weaknesses as well as their components [78]. As a result of this review of different e-voting models, a secure remote e-voting model was developed to meet the requirements of Tanzania citizens.

To operate the system, National Election Commission should first publish a set of voting client applications that can run on all the available operating system platforms. Kimbi and Zlotnikova[78]proposed applications for Windows, Linux and Mac OS to be available in order to allow a good number of voters using different operating systems to participate in elections. The application should be downloaded from the secure website that has to be maintained by National Election Commission. To ensure votes authentication, secrecy and integrity of the votes, the authors adopted the double envelop scheme from the Estonian model[78].

The proposed model [78]is equipped with the use of three-factor authentication with a biometric fingerprint scanner to accept a scan, recognize the voter, and open the correct voter record in the database and verify the voter. This module uses a dynamic link library (DLL) that can be displayed in a web application. This allows the voter's biometric data to be read by a web application and sent to a web service for verification. According to [15], a voter does not have to claim an identity and the e-voting system takes on the burden to identify her.

This will lead to an increased load on the servers when applied on a large scale. To improve this is to make the voter specify a district where he is registered to minimize the system load. Once more, authors only presented the verification method using fingerprint while neglecting the whole e-voting system security issues such as encryption of the vote while travelling through unsecure channels such as the Internet as this is the only communication channel on the proposed system [78].

2.7.5 Helios Electronic Voting Model

According to [16], the Helios Electronic voting model [60] is a simplified online voting system, which can be used by anyone, from anywhere and without restrictions to geographical locations. It is a web-based open audit system developed by Harvard University and Adiba [62]. The model was built on existing web programming technologies and cryptographic voting protocols that use the Google App Engine to run the voting application as well as the ElGamal cryptographic and anonymization mechanisms to provide voter secrecy [12]. The system also allows voters to track ballots, and makes it easy for the public to verify the final results, as it allows open election audit[60]. It focuses mainly on public interest and computer literacy [60],[62].

The voting system is open to new possibilities of verifying and auditing ballots cast over the Internet. The Helios voting system allows anyone to create an election, invite voters to cast secret ballots electronically, compute a tally and then generate a valid proof of the entire process [16].

The Helios voting model defines voting systems targeting low-coercion election without putting high risks at stake (student elections, organization etc.)[12]. It does not assume the threat of potential external attack to be very high, and this means that attack prevention relies only on auditing. The cryptographic protocol adopted by this system does not prevent ballot stuffing by external attackers[12]. Only individual voters can check the validity of cast ballots, and if the server is corrupt, ballot stuffing or impersonation can occur forthright even before the election ends. The Helios model also accepts the risk that if the server is compromised before the end of elections, it could negatively impact the secrecy of the ballot.

The Helios voting model is vulnerable to attacks such as voter impersonation. Therefore, when the Helios voting system is being corrupted, ballots of all the voters could be revealed to hackers or intruders, who could manipulate the cast ballots leading to incorrect voting results. The developed model tries to solve the encountered problems by introducing strong authentication mechanisms and the integrity of the cast ballot is verified through the entire voting process, without letting any content of the ballot to be associated with any voter. The developed approach will allow communication between the client side and the voting server over an insecure channel with minimal threats, and ensure that only one vote is counted per voter, rendering ballot stuffing impossible at all times.

Table 3.0.1 Summary of characteristics of similar E-voting Models

No.	Author(s) and System Year	Methodology/Features	Strength of Method	Limitation of Method
1	Muhammad and Oluwafeni, 2016[76]	Uses 3-tier architecture, client, server, and database tiers, with authentication achieved via ID and password. It also give voters an option offline and online	Provides voters with a platform to either vote online and offline for those without computer or internet	Application of mobile platform only would imply that the success of the election would have to primarily rely on mobile service providers. It is also expensive to adopt in developing countries with financial crisis
2	Molokwu and Agu, 2014 [77]	System employs three agents, a ballot distributor, certifying authority, and vote compiler, and public key encryption	Supports adequate requirements including accuracy, democracy, privacy and verifiability	• Cannot prevent vote buying • Poor fraud detection, and • Cast ballot can be traced back to voter
3	Olaniyi <i>et al.</i> 2012 [75]	Uses multifactor authentication and cryptographic hash function	Ensures the integrity of voting process and data	Uses a centralized server which creates a single point of attack against voting data.
4	Kimbi, Sylvester; Zlotnikova, Irina, 2014 [78]	Uses three-factor authentication with a biometric fingerprint scanner for authentication and voter verification	Ensure verifiability and authentication	Uses a centralized server which creates a single point of attack against voting data

5	Adida,Ben 2008, [16]	Uses the ElGamal cryptographic and anonymization mechanisms to provide voter secrecy	Ensures the integrity of voting process and data	Suitable only for Student Representative Council, therefore cannot be used for general/presidential elections.
6	M.O Yinyeh , K.A. Gbolagade, 2013, [79]	Uses finger prints, passwords and Personal Identification Numbers to provide user authentication and validation	Ensure authentication and validation of users	The architecture would not support the principle of secrecy of elections. Encryption scheme used not discussed.

2.8 Conclusion on Literature review

Based on the existing literature, this study was able to identify security challenges from atechanical perspective that hinder the adoption and implementation of secure and accurate voting systems. This chapter also identifies limitations and gaps which act as critical factors leading to poor voter turnouts. These limitations includelack of secret protection measures, compromised voter computers and coercion. It also identifies security requirements that secure remote voting systems should comply with or what developers should do in order to come up with secure voting systems. These requirements are in line with general principles of democratic elections. The literature has proven that for a voting system to be successful and to gain voter's trust, it should ensure that proper security controls are implemented. Additionally, most of the discussed and reviewed systems and models are subjected to various security threats. These threats are, (1) denial of services, (2) vote stuffing, buying and coercion, (3) and web spoofing (*see subsection 2.3.7*). These can lead to voters losing trust and confidence in using the modern way of voting (e-voting).

We also reviewed and analyzed several voting systems and models which can be used to develop secure voting systems based on cryptographic mechanisms. Based on the foregoing, weobservedthat a mechanism which combines cryptographic techniques and E2E mechanism such as used in Estonia (*subsection 2.2.1.1*) and Norwegian (*subsection 2.2.1.4*) voting models would be most appropriate for a secure and trustable voting system. The two models will be enhanced to complement each other and be customized to meet necessary

requirements. Our model will adopt the envelope technique discussed in *sub-section 2.5* used within the Estonian model and the ElGamal discussed in *sub-section 2.4.2* digital signature scheme adopted by Norwegian model will be replaced with RSA digital signature scheme discussed in *sub-section 2.6*. For authentication, the proposed model uses three factor authentication mechanism for identification and authentication of eligible voters. This will be made possible by using Public Key Infrastructure (PKI) and a National Identification Number (ID card). Before voters can cast their votes, they have to be provided with e-ID cards with PKI capabilities.

According to the reviewed literature, the remote electronic voting system needs to comply with all the principles of democratic elections[4],[36]. Remote electronic voting systems need to be trustworthy, secure and as reliable as a traditional democratic election[33],[38]. In particular, for a voting system to be secure it needs to, (1) keep all ballots secrets, (2) ensure accuracy of the system without errors or interference, (3) achieve democracy by allowing only one valid voter to cast one vote, (4) provide individual and universal verification to ensure that ballots are tallied correctly, (5) ensure that the system is available and accessible to all voters, (6) and lastly the system should not disclose results before the election closes[30],[36],[80].

CHAPTER 3

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

In this chapter we present the research design and discuss suitable research paradigms needed for collecting and analyzing research data. It further covers the steps taken when gathering and analyzing data, and as well as validity and reliability of the study. This research adopted descriptive research design to describe the views and experience of voters concerning current voting system.

3.2 Research Design

The research design is defined as a blueprint for conducting a study that increases the probability that the study findings are a true reflection of reality [63]. Burns and Grove [63] further clarify that clues to the appropriate research design are found in the research purpose, framework, research objectives, questions and hypothesis. A descriptive study design with mixed-method approach was adopted in this research in order to describe the experience and views of voters concerning the current system used for electing candidates. According to [81],[82], there are three types of data collection methodology: qualitative (interview and observational data), quantitative (numeric data), and mixed method (uses both type of data). The mixed method covers the benefits of both methods [83],[84].

A mixed method, is defined as a methodology used for conducting research that involves collecting, and analyzing of data by integrating qualitative and quantitative research within a single study [10],[82],[85],[86]. The purpose for combining the two methods is to get a better understating of the research problem or a phenomenon under study [81],[82],[84]. In order to satisfy the objectives of this research, we adopted mixed methods approach because of its capabilities of solving the weaknesses of one method using another method's strengths. The qualitative method is more appropriate for smaller samples [81],[85] and can be perceived to

limited in reflecting the opinions of a larger population[81], therefore qualitative method was used to collect data from a small sample of election and security experts. However, for collecting data from a large population of respondents (voters) quantitative method was adopted.

3.2.1 Descriptive Research Design

According to [63], descriptive research design studies are designed to gain more information about a phenomenon as it naturally occurs. It is designed to develop theories, identify problems with current practices or determining what other researchers are doing in similar situations [63]. For the purpose of this research, after examining the objectives of this research, this thesis adopts exploratory research design to give answers to the raised research questions and its objectives.

3.2.2 Quantitative and Qualitative approach

Qualitative approach employs an inductive approach in which the researcher first collects data and then attempts to drive explanations from those data. It tends to be more exploratory in nature by seeking to provide insight into how individual or organizations understand aspects of their world or the given context[63]. This approach is based on the wider view that there is no single reality, but rather that perceptions defer from one person to another over time and what is known has a meaning only within a given context[63].

Qualitative research is concerned about understanding social phenomena based on respondent's point of view[63]. For this research, qualitative technique was used to gain the in-depth understanding of the current problems associated with voting in Botswana by interviewing security and election experts (IEC) and also to get their point of view on the idea of introducing e-voting within their organization.

A quantitative approach refers to numerical data or information that can be converted into numbers, and involves experimental control to quantify phenomena[10],[63]. This method was adopted for this research to measure beliefs from security and election experts, and voters about the current paper-based voting system used in Botswana. Therefore, the feedback from participants will be used to design a secure model which matches the beliefs of all the

participants. The questionnaire method was used to collect the quantitative type of information from voters.

3.2.3 Methods used to attain Objectives

In this sub-section, the specific methods used to achieve specific objectives are presented.

3.2.3.1 First Objective *“To identify potential benefits of introducing remote e-voting in Botswana”*

The first objective was achieved by using mixed research method. Diverse experience of different experts (respondents) with different perceptions on the topic under study were put together to give the researcher a complete picture of how voters and security experts perceive the benefits of introducing a remote electronic voting system in Botswana. The feedback from voters and experts concerning their perceptions on the introduction of remote e-voting system gave us a broader picture on how they perceived e-voting system. All these aspects were included to understand the necessity for introducing a remote electronic voting system in Botswana.

Due to the complexity of the phenomenon under study, the data collected was difficult to quantify alone, and therefore mixed research method was adopted to give appropriate answers to the research question.

3.2.3.2 Second Objective *“To identify security challenges from a technical perspective that hinder the introduction and implementation of online voting in Botswana”*

The second objective was attained through the use of content analysis. According to [86],[87] content analysis can be defined as a research tool that can be used to determine the presence of certain keywords or a concept within a given set of text. Content analysis provides new insights, and increases a researcher's understanding of a particular phenomenon [86]. Inductive content analysis was used to get the relevant information from the respondents, because according to the findings from this study, they were no researches similar to this research in Botswana, which aims at designing an e-voting model to reduce the problem of poor voter turnout. According to Elo and Kyngas [86], inductive content analysis can be used in situations whereby there are no previous studies dealing with the phenomenon or when it is

fragmented. Therefore, we were able to easily identify the problems and loopholes from the existing solutions and also to establish challenges hindering the adoption of electronic voting systems in Botswana. The data was collected using perception analysis forms (questionnaires) from security and election experts (quantitative) and qualitative technique using interviews.

3.2.3.3 Third Objective *“To identify security requirements of a secure online voting system”*

The third objective was achieved through the use of deductive content analysis. Deductive content analysis, is normally used when the phenomenon or structure of analysis is based on previous knowledge [86], [87]. We reviewed similar studies trying to give solutions to the topic under study. We also interacted with security experts to get their perceptions on security requirements for secure voting systems through the use of perceptive analysis forms (questionnaires).

3.2.3.4 Fourth Objective *“To develop a conceptual voting model for designing and implementation of secure and trusted remote voting system that can be used and adopted for future general elections in Botswana”.*

The fourth objective was achieved through the use of desk review technique and the results from the findings. We reviewed several similar voting systems and models, then analyzed them, identified their strengths and weaknesses together with their components (databases, algorithms and cryptographic mechanisms) adopted. The secure conceptual model was therefore developed from a combination of critical success factors from similar systems and models studied, as well as the additional knowledge acquired and the feedback obtained from security experts. The responses from the respondents pertaining to challenges hindering considerations to introduce e-voting in Botswana were taken into consideration when developing the proposed model.

3.3 Research population and sampling

3.3.1 Research Population

According to [63], research population is the entire set of individuals that meets the sample criteria of the study. BIUST undergraduate students were used as targeted population to collect

primary data. The population also included the security and election experts from the Botswana International Electoral Commission.

3.3.2 Sampling

For the proposed research, a purposive sampling technique was adopted to select the required research sample. The purposive sampling method is defined as a method which involves conscious selection of certain respondents to gain insight or obtain an in-depth understanding of complex experiences or events [63],[88]. Brink [10] further defines a sample as a fraction of the whole population selected by the researcher to participate in the study. There were 30 security and election experts, and 300 voters who participated in this study. The advantage to this technique is that it allowed for selection of respondents based on their skills and knowledge to gain rich and relevant data.

3.3.3 Sample size

The study sample was drawn from three different types of respondents, being voters (both illiterate and literate), security, and election experts. Questionnaires were given to voters to collect their perceptions towards using the manual paper-based voting system. The *table 3.0.1* shows an estimated number of respondents within BIUST and IEC officers. The security and election experts were also consulted to help the researcher with procedures followed when conducting general elections, and provide the perceived security requirements for secure voting systems.

3.4 Data collection

The researcher collected and stored multiple sources of the evidence systematically and comprehensively. The following research methods were used in this research to collect relevant data.

3.4.1 Questionnaire and interview

We used questionnaires to collect, gather, analyze and determine voter's views and opinions about the current paper-based voting method, as well as the idea of introducing remote e-

voting in Botswana. Two different sets of questionnaires were given to both voters and experts. An online survey link (<https://docs.google.com/forms/d/1dTO6aBizFwkkVWCMvAwv-X0elPNB63tIYf4dHIPd3jU/edit>) was sent to all voter respondents via e-mail, and each was afforded ample time to respond. However, the security experts were also furnished with hard copies of the questionnaire, which were distributed to selected centers, which include Palapye, Serowe, Mahalapye, and Gaborone. The Botswana IEC top officials were also interviewed about the current state of the paper-based system in place and their perceptions on the idea of introducing remote e-voting in Botswana.

The Likert scale in *table 3.0.1* was used as it appears which rendered it easy for respondents with varying degrees of educational backgrounds to attempt. Likert scale was used because it is easy to understand and work with [10], [86].

Range	Interpretation
1	Strongly Agree
2	Agree
3	Neutral
4	Disagree
5	Strongly Disagree

Table 3.0.2 Likert Scale

3.4.2 Secondary Data

Secondary data was also used to gather relevant information from existing systems and models developed by different depositories. Different voting models were reviewed and analyzed to identify their strengths and weaknesses as well as their components. This helped to easily identify the security requirements for a secure remote electronic voting system and also to upgrade our background knowledge within the area under study.

3.5 Questionnaire Design

All the questions included in the questionnaire were made simple to understand and easy to answer, especially because of the respondent's varying educational levels. To achieve all this, we issued out a pilot study to 30 different respondents (including IEC experts and voters) of differing social and educational backgrounds in Palapye. Respondents were given a Likert scale table as in *table 3.0.2* for answering most of the questions.

3.6 Data processing and Analysis

During the study, the quantitative method was used to analyze the data collected through the use of perception analysis forms (questionnaires) and the results were presented in graphs and tables. Microsoft excel was also used to generate graphs from respondent's results.

3.7 Reliability and Validity

3.7.1 Reliability

According to [89], refers to reliability as the degree of consistency with which an instrument measures the attribute it is designed to measure. According to [88], they further describe reliability as the way how researchers are consistent with their way of recording, analyzing, and interpreting data in order to extract meaning from the given data.

For this research, reliability was influenced by the relationships between the researcher and the respondents. We explained our role in the study to the respondents as required, to ensure that our presence does not influence reliability. According to [88] and [89], reliability can be influenced by the settings and social context. Therefore, questionnaire was distributed to the respondents who in turn were afforded freedom to answer questionnaires at their own pace. Item analysis was conducted to determine the internal consistency and reliability of each individual item as well as each subscale.

3.7.2 Validity

According to [88], research validity can be referred to as an extent to which the information collected is perfect and truly represents an accurate picture of what is being studied. Internal validity can be referred to as the degree to which the explanation of phenomena matches the realities found within the given context or of the world [88]. In particular, validity refers to the extent to which the findings of the given study or topic is correctly described. With this research, validity was achieved through the problem being investigated, and the objective of the problem. During the interview, we requested for clarifications and summarized interviews to make sure that responses are understood and to ensure that the interviewer had an accurate understanding of what respondents said. The questionnaires were made simple for easy comprehension by every respondent.

3.8 Conclusion

A descriptive design with mixed methods (qualitative and quantitative) was adopted for this study. Security and election experts, and voters were selected as the targeted population. The sample was selected using purposive sampling technique. The researcher selected 330 respondents according to a self-formulated sampling criteria, of which 30 respondents were security and election experts and 300 respondents representing voters. Questionnaires were distributed to voluntary respondents to answer at their convenience. Respondents were also granted an opportunity to withdraw at any time. The Likert scale was used to interpret responses of each respondent.

The statistical data analysis tools used and methods used to attain each objective are also presented in this sub-chapter. Secondary data was used to gather relevant information from existing systems and models developed by different depositories. The following chapter presents an in-depth description of data analysis and interpretation.

CHAPTER 4

RESULTS ANALYSIS AND INTERPRETATION

In this chapter we present results of the findings and data analysis. The data was analyzed to describe perceptions and experiences of IEC employees and voters concerning the paper-based voting system used in Botswana. The targeted group included voters, security and election experts. There were 330 questionnaires distributed, and only 227 responses were received, 200 copies were received from voters and 27 copies were received from IEC employees. The sub-section below gives data analysis and interpretation of the findings.

4.1 Findings from Security and Election Experts (IEC)

This sub-section give analysis and interpretation of data collected from IEC employees.

4.1.1 Description of sample

All the 27 respondents were citizens of Botswana eligible to vote and were employed by IEC. The characteristics of the sample are presented in Tables.

Demographic data

This sub-section shows demographic data of respondents, which include gender, age, and educational background.

Gender			Age		
	Frequency	Percentage		Frequency	Percentage
Female	9	33%	25– below	7	26%
Male	18	67%	26 - 35	12	44%
Total	27	100%	36 and above	8	30%
			Total	27	100%

Table 4.0.1-Gender and age range

Table 4.0.1 shows that most respondents were male. Most of the respondents were aged 26-35 years.

Educational Level			Work Experience		
	Frequency	Percentage		Frequency	Percentage
High school or less	7	26%	Above 10 years	13	48%
Certificates and Diploma	8	30%	6 – 10 years	10	37%
Bachelor's degree	10	37%	1 – 5 years	4	15%
Master's degree	2	7%	Total	27	100%
Total	27	100%			

Table 4.0.2 - Education Level and Work experience

According to **table 4.0.2** it is evident that most IEC security and election experts are Bachelor's degree holders. The largest ratio has above 10 years work experience.

	Frequency	Percentage
Admin Officer	10	37%
IT Officer	9	33%
System Analyst	5	19%
Top Level Management	3	11%
Total	27	100%

Table 4.0.3 Position

Table 4.0.3 shows that the largest ratio of respondents are employed as administration officers with a percentage of 37%.

4.1.2 Accessing the current Situation

This sub-section presents respondent's ideas and views about the e-voting system.

Q6.*How do you rate your level of understanding about e-voting systems?*

	Frequency	Percentage
Very high	8	30%
High	10	37%
Medium	3	11%
Low	4	15%
No knowledge	2	7%

Table 4.0.4 - Level of understanding of e-voting system

The results from **table 4.0.4** show that 93% (very high, high, medium and low) of respondents have a positive understanding of e-voting.

Q7.*According to your personal opinion, do you think the current paper-based system has problems?*

	Frequency	Percentage
Yes	20	74%
No	7	26%

Table 4.0.5 Current System Problems

It can be observed from **table 4.0.5** that the largest ratio of 74% agreed with the submission.

Q8.*Do you believe that e-voting can reduce election problems in Botswana?*

	Frequency	Percentage
Yes	18	67%
No	3	11%
Not Sure	6	22%

Table 4.0.6- Can e-voting reduce election problem in Botswana?

Table 4.0.6 shows that out of 27 respondents, the largest ratio of respondents agreed with the submission.

Q9. *Are you willing to use an e-voting system if introduced in Botswana?*

	Frequency	Percentage
Yes	25	93%
No	2	7%

Table 4.0.7 - *Willingness to use an e-voting system*

According to **table 4.0.7**, most of the respondents are willing to use the e-voting system if introduced in Botswana.

4.1.3 Potential Benefits of introducing an e-voting system in Botswana

This sub-section focuses on capturing perceptions of respondents on what they think can be potential benefits of introducing an e-voting system in Botswana whose results have been published below.

Q10. *Would E-Voting increase voter turnout if introduced?*

	Frequency	Percentage
Strong Agree	-	-
Agree	7	26%
Neutral	3	11%
Strongly Disagree	10	37%
Disagree	7	26%

Table 4.0.8 - *Voter turnout*

As can be seen from **table 4.0.8**, most of the respondents disagreed that introducing e-voting would increase voter turnout.

Q11. *Would E-voting eliminate delays in ballot counting?*

	Frequency	Percentage
--	-----------	------------

Strong Agree	19	70%
Agree	5	19%
Neutral	3	11%
Strongly Disagree	-	-
Disagree	-	-

Table 4. 0.9- Eliminate delays in ballot counting

Table 4.0.9 shows that the largest ratio of respondents strongly agreed that introducing e-voting would eliminate delays during vote counting.

Q12.*Would E-voting prevent election fraud (vote rigging, multiple voting, and results manipulation)?*

	Frequency	Percentage
Strong Agree	6	22%
Agree	15	56%
Neutral	4	15%
Strongly Disagree	2	7%
Disagree	-	-

Table 4.0.10- Prevention of election fraud

According to **table 4.0.10** it is evident that most respondents agreed that e-voting would prevent and eliminate election fraud.

Q13.*Would E-voting speed-up the voting process?*

	Frequency	Percentage
Strong Agree	20	74%
Agree	7	26%
Neutral	-	-
Strongly Disagree	-	-
Disagree	-	-

Table 4.0.11- Speeding-up the voting process

Based on the results from **table 4.0.11**, it shows that all the respondents believe that introducing e-voting would speed up the voting process.

Q14. *Would E-voting eliminate voting errors due to wrong markings?*

	Frequency	Percentage
Strong Agree	10	37%
Agree	17	63%
Neutral	-	-
Strongly Disagree	-	-
Disagree	-	-

Table 4.0.12–*Elimination of Voting Errors*

Table 4.0.12 shows that all the 27 respondents agreed that introducing e-voting would eliminate voting errors by voters.

Q15. *Would E-voting eliminate ballot counting errors due to manual counting?*

	Frequency	Percentage
Strong Agree	7	26%
Agree	18	67%
Neutral	2	7%
Strongly Disagree	-	-
Disagree	-	-

Table 4.0.13- *Elimination of Ballot Counting Errors*

Table 4.0.13 shows that all the respondents agreed that e-voting would eliminate ballot counting errors due to manual counting.

4.1.4 Potential Challenges of introducing E-voting system

Technical challenges

Q16. *IEC staff do not have enough skill set to support and manage implementation of e-voting?*

	Frequency	Percentage
Strong Agree	5	19%
Agree	11	41%
Neutral	5	19%
Strongly Disagree	2	7%
Disagree	4	15%

Table 4.0.14- IEC Staff Skill

Table 4.0.14 shows that most of the respondents believe that IEC staff do not have enough skill to support and manage implementation of e-voting.

Q17. *Is there lack of ICT resources by IEC to support introduction and implementation of E-voting system?*

	Frequency	Percentage
Strong Agree	5	19%
Agree	15	56%
Neutral	3	11%
Strongly Disagree	3	11%
Disagree	1	4%

Table 4.0.15 - Lack of ICT resources

Based on **table 4.0.15**, it shows that out of 27 respondents, most respondents agreed that the IEC does not have enough resources to implement e-voting.

Q18. *Would there be unstable communication link during the election period?*

	Frequency	Percentage
Strong Agree	2	7%
Agree	19	70%
Neutral	4	15%
Strongly Disagree	2	7%
Disagree	0	0

Table 4.0.16- *Unstable communication link during election period*

As can be observed from **table 4.0.16**, most respondents believed that there would be lack of communication to people living in rural areas during election period.

Q19. *Could an E-voting system fail during election days due to system failure or software bugs?*

	Frequency	Percentage
Strong Agree	6	22.2%
Agree	19	70.4%
Neutral	2	7.4%
Strongly Disagree	0	0
Disagree	0	0

Table 4.0.17- *E-voting system failure during election period*

According to **table 4.0.17**, it is evident that most respondents agreed that there would be a failure of the system during the election period.

Q20. *An outage of electricity during election period would disrupt smooth elections?*

	Frequency	Percentage
Strong Agree	7	26%
Agree	20	74%
Neutral	0	0
Strongly Disagree	0	0
Disagree	0	0

Table 4.0.18- *Outage of electricity during election period*

Based on **table 4.0.18**, it shows that all the respondents agreed that the problem of power disruption especially in rural areas would be a big problem.

Q21. *There would be security issues due to intruders and hackers hacking into the system and manipulating vote results?*

	Frequency	Percentage
Strong Agree	0	0
Agree	17	63%
Neutral	3	11%
Strongly Disagree	2	7%
Disagree	5	19%

Table 4.0.19- Security issues

Table 4.0.19 shows that most respondents believe that security of the e-voting system can be a concern as hackers can attack the system and manipulate the election results.

General challenges

Q22. *The cost of introducing and implementing e-voting would be high?*

	Frequency	Percentage
Strong Agree	5	18.5%
Agree	15	55.6%
Neutral	5	18.5%
Strongly Disagree	0	0
Disagree	2	7.4%

Table 4.0.20- The cost of implementing e-voting system

Based on **table 4.0.20**, it is evident that most respondents perceived that the cost of introducing e-voting will be high.

Q23. *E-voting would be difficult to use due to high illiteracy rate?*

	Frequency	Percentage
Strong Agree	7	25.9%
Agree	13	48.1%
Neutral	5	19%
Strongly Disagree	0	0

Disagree	2	7%
----------	---	----

Table 4.0.21- High illiteracy rate

Table 2.0.21 shows that out of 27 respondents, most respondents agreed that illiteracy rate among voting populace would be a major problem when introducing and implementing e-voting system.

Q24. *The difficulty for voters to confirm that how they voted is what is recorded by the system?*

	Frequency	Percentage
Strong Agree	2	7%
Agree	19	70%
Neutral	4	15%
Strongly Disagree	2	7%
Disagree	0	0

Table 4.0.22- Would voters be able to confirm their votes?

Q25. *Would voters find the user interface cumbersome to use?*

	Frequency	Percentage
Strong Agree	4	15%
Agree	10	37%
Neutral	6	22%
Strongly Disagree	3	11%
Disagree	4	15%

Table 4.0.23 E-voting user interface

4.2 Findings from voting populace (voters)

This sub-section presents data analysis and interpretation of responses from voters.

4.2.1 Description of sample

Demographic information

Gender			Age		
	<i>Frequency</i>	<i>Percentage</i>		<i>Frequency</i>	<i>Percentage</i>
Female	140	70%	25 – below	160	80%
Male	60	30%	26 – 35	22	11%
Total	200	100%	36 and above	18	9%
			Total	200	100%

Table 4.0.24 - Gender and Age

From **Table 4.0.24** we observed that out of 200 respondents, majority were female. The largest number were below 25 years.

	Frequency	Percentage
High school or less	190	95%
Certificates and Diploma	10	5%
Bachelor's degree	0	0
Master's degree	0	0
Total	200	100%

Table 4.0.25 - Education

As can be observed from **table 4.0.25**, most of respondents are high school certificate holders. This is particularly because the sample consisted predominantly of undergraduate students.

4.2.2 Assessing the current situation and problem

This sub-section assesses the current situation and also seek to determine the type of voting technology voters would prefer to use for future general elections.

Q4.*Have you ever voted in any general elections in Botswana?*

	Frequency	Percentage
Yes	150	75%
No	50	25%

Table 0.26- *Past participation in any general election*

As can be observed from **table 4.0.26**, most of voters had voted before in general elections.

Q5.*Have you ever heard of an e-voting system?*

	Frequency	Percentage
Yes	195	97%
No	5	3%

Table 4.0.27- *Have you ever heard of e-voting?*

Based on **table 4.0.27**, it shows that most respondents had heard about e-voting systems.

Q6. *In your opinion, do you think the current paper-based voting system has problems?*

	Frequency	Percentage
Yes	175	87%
No	15	8%
Not sure	10	5%

Table 4.0.28- *Opinion on current system*

Table 4.0.28 shows that over 87% out of 200 respondents, believe that the current traditional paper-based voting system has problems.

Q7. *Do you believe e-voting can reduce election problems in Botswana?*

	Frequency	Percentage
Yes	150	75%
No	30	15%
Not sure	20	10%

Table 4.0.29- *Can e-voting solve election problems in Botswana?*

Based on results in **table 4.0.29**, 75% of the 200 respondents, believe that introducing e-voting will reduce election problems in Botswana associated with the traditional paper-based voting system.

Q8. *Do you think it is necessary to introduce an e-voting system in Botswana?*

	Frequency	Percentage
Yes	180	90%
No	15	7.5%
Not sure	5	2.5%

Table 4.0.30- *E-voting introduction*

Table 4.0.30 shows most respondents think it is necessary to introduce e-voting in Botswana.

Q9. *Are you willing to use an e-voting system if introduced in Botswana?*

	Frequency	Percentage
Yes	185	92%
No	10	5%
Not sure	5	3%

Table 4.0.31- *Willingness to use an E-voting system*

Table 4.0.31 shows that most respondents would be willing to use an e-voting system if introduced.

Q10.*Can you rely on and trust the results of an e-voting system?*

	Frequency	Percentage
Yes	187	93%
No	10	5%
Not sure	3	2%

Table 4.0.32– *Reliance on the results of an E-voting system*

According to **table 4.0.32**, it is evident that most of respondents agreed that they can rely on the results of an e-voting system.

Q11.*What voting technology would you prefer?*

	Frequency	Percentage
Paper-Based voting	30	15%
E-voting	170	85%

Table 4.0.33- *Voting technology of choice*

As can be observed from **table 4.0.33**, it is evident that most of respondents would prefer using e-voting over a traditional paper-based voting system.

Q12.*What is the level of your computer experience?*

	Frequency	Percentage
Expert	30	15%
Advance	80	40%
Average	70	35%
Basic	15	7%
No experience	5	3%

Table 4.0.34- *Computer experience*

According to **table 4.0.34**, more than 90% of the 200 respondents, have basic experience using computers.

4.2.3 Potential Benefits of introducing e-voting system in Botswana

This sub-section focuses on capturing perceptions of respondents on what they think can be potential benefits of introducing an e-voting system in Botswana with the results presented in the preceding tables.

Q13. *Would E-voting increase voter turnout if introduced?*

	Frequency	Percentage
Strong Agree	94	47%
Agree	60	30%
Neutral	26	13%
Strongly Disagree	15	7.5%
Disagree	5	2.5%

Table 4.0.35- *Voter turnout*

Based on results in **table 4.0.35**, more than 70% of the 200 respondents, believe that introducing e-voting would increase voter turnout.

Q14. *Would E-voting eliminate delays in ballot counting?*

	Frequency	Percentage
Strong Agree	94	47%
Agree	60	30%
Neutral	26	13%
Strongly Disagree	15	7.5%
Disagree	5	2.5%

Table 4.0.36- *Eliminate delays in ballot counting*

Q15. *Would E-voting prevent voting fraud (multiple voting, votes manipulation etc.)?*

	Frequency	Percentage
Strong Agree	94	47%

Agree	60	30%
Neutral	26	13%
Strongly Disagree	15	7.5%
Disagree	5	2.5%

Table 4.0.37- Voting fraud

Based on results in **table 4.0.37** it is evident that more than 70% of the 200 respondents, believe that e-voting would prevent/reduce fraud.

Q16. Would E-voting speed-up the voting process?

	Frequency	Percentage
Strong Agree	93	46.5%
Agree	107	53.5%
Neutral	0	0
Strongly Disagree	0	0
Disagree	0	0

Table 4.0.38- Speed-up voting process

From **table 4.0.38** it can be seen that all respondents believe that introducing e-voting would speed-up the voting process.

Q17. Would E-voting eliminate voting errors?

	Frequency	Percentage
Strong Agree	100	50%
Agree	71	35.5%
Neutral	29	14.5%
Strongly Disagree	0	0
Disagree	0	0

Table 4.0.39– Elimination of voting errors

It can be observed from **table 4.0.39** that more than 80% of the respondents believe that e-voting would eliminate voting errors if correctly implemented.

Q18. *Would e-voting eliminate ballot counting errors associated with manual counting?*

	Frequency	Percentage
Strong Agree	77	48.5%
Agree	73	36.5%
Neutral	23	11.5%
Strongly Disagree	17	8.5%
Disagree	10	5%

Table 4.0.40- *Eliminate ballot counting errors*

According to **table 4.0.40**, most of respondents agreed that e-voting system would eliminate ballot counting errors due to manual count.

4.2.4 Potential challenges of introducing E-voting in Botswana

This sub-section focuses on capturing perceptions of respondents on potential benefits of introducing the e-voting system in Botswana with the results shown below.

Q19. *I do not think e-voting is appropriate since I do not believe the vote will be kept a secret?*

	Frequency	Percentage
Strong Agree	21	10.5%
Agree	13	6.5%
Neutral	26	13%
Strongly Disagree	76	38%
Disagree	64	32%

Table 4.0.41- *Is E-voting appropriate?*

As it can be observed from **table 4.0.41**, it is evident that respondents disagreed that e-voting introduction is not appropriate.

Q20. *E-voting is not appropriate because of security reasons (insiders and hackers can easily hack into the system and manipulate votes)?*

	Frequency	Percentage
Strong Agree	6	3%
Agree	13	6.5%
Neutral	16	8%
Strongly Disagree	76	38%
Disagree	89	44.5%

Table 4.0.42- *e-voting security issues*

The **table 4.0.42** shows that most respondents disagreed that e-voting is not appropriate because of security reasons.

Q21.*The voter can easily confirm their ballot has been recorded-as-cast, recorded-as-tallied.*

	Frequency	Percentage
Strong Agree	11	5.5%
Agree	14	7%
Neutral	21	10.5%
Strongly Disagree	89	44.5%
Disagree	65	32.5%

Table 4.0.43- *Can voters confirm their ballot?*

As can be seen from **table 4.0.43**, most respondents disagreed with the submission.

4.3 Responses from Interviews with security and election experts (IEC)

In this sub-section we present the results of the interviews conducted with security and election experts to get their views and professional opinions on the current state of the paper-based voting system adopted and perceptions on the idea of introducing an e-voting system in Botswana.

Question 1. In your professional opinion, do you think the current paper-based voting system has problems?

According to the responses it shows that the current system has problems that leads to poor voter turnout. Some of the problems are long queues and the time taken by individual persons to cast their ballot. As a result some of the voters tend to leave the voting stations before they have had an opportunity to cast their ballot especially the young generation and employed people.

“Personally, I think the current paper-based voting system used in Botswana has problems which normally leads to poor voter turnout due to long queues, and the length of time it takes for one to cast their ballot” [Respondent 1].

“Normally voters end up leaving the voting stations and go home before casting their votes, some even never show up due to these problems, most of the cases young Batswana (or youth) or employed people never or few of them show up during registration and election period” [Respondent 2]

The other expert mentioned that a person who stays in Gaborone and other cities and towns because of jobs and schools, their home villages are as far as Maun, Gantsi, and Shakawe, therefore it is difficult for them to participate during elections due to transportation logistics and financial resources. They further said the current system does not make a provision for voters to correct their voting choice, since multiple marks lead to a spoilt ballot.

“The other problem with this system, is that it is not easy to correct the mistake because if you cancel and opt for the second time it means the ballot paper has been spoilt or one has to request for the new ballot paper” [Respondent 3]

“Appointed poll staff may be engaged for longer periods and they may be exhausted and make mistakes” [Respondent 4]

Question 2. What are the potential benefits of introducing remote e-voting system in Botswana?

The responses show that respondents perceived that introduction of a remote e-voting system will bring benefits. One respondent mentioned that introducing a remote e-voting system will reduce the chances of spoilt votes due to wrong markings, eliminate time consumed by manual counting, eliminate tallying errors occasioned by manual counting, even speed up the voting process and reduce long queues thereby attracting more youth and those who work to take part during elections.

“E-voting will reduce the chances of spoilt ballots due to wrong markings, it will eliminate time taken when counting ballots and errors made due to manual counting, and even speed up the voting process as long queues will be reduced and attract more youth and working people” [Respondent 1]

The other respondent felt that it is necessary for Botswana to introduce remote e-voting, although she is currently not ready and beset by a multitude of challenges that hinder adoption and implementation of a remote e-voting system, the likes of which are a populace that is psychologically unprepared to accept such a system, poor educational background and general lack of appreciation of new technologies. However, he felt that training and education could alleviate such problems. He further alluded that introducing an e-voting system would reduce cost of running election in Botswana as less officials at poll stations will be required.

“I think Botswana like other countries, it will have to introduce remote e-voting to replace the current system in future. Though most of Botswana are not ready emotionally, and their educational background is still poor concerning the use of technology most especially those in rural areas, but they will have to be educated of course.” [Respondent 2]

“Remote e-voting will make the cost of running elections cheap and affordable as less polling officers will be required” [Respondent 3]

Question 3. What are the potential challenges that hinder implementation of remote e-voting in Botswana?

Based on the responses from respondents, it shows that there are existing challenges that would hinder introduction of remote e-voting system in Botswana. One respondent mentioned that some of the problems that would hinder introduction of a remote e-voting system include, high rate of computer illiteracy and power shortage in rural areas, and the perceived security of a remote e-voting system. He further perceived that cast votes and voter's privacy will not be protected to that standard required by IEC. The other respondent perceived that the cost of implementing e-voting system would be high, and that the current ICT infrastructure of the IEC is not to the standard to run and maintain an e-voting. Therefore, it would be hard to introduce such a system unless improvements are made on the system infrastructure.

“The reason why remote e-voting system is not implemented in Botswana include, the high cost of implementing e-voting, but we think if we are to implement a new voting system we believe our organization can be supported by the government and other parastatals” [Respondent 1]

“The ICT infrastructure for our organization was designed only to cater for the current system, therefore it will be hard for us to implement or introduce a new voting system, unless we upgrade the existing system” [Respondent 2]

Another respondent mentioned that other critical security issues are aligned with attacks such as client-side attack because electronic devices such as phones and computers are vulnerable to viruses and malicious software which can impersonate voters. He further said the other attack can be found at the server side, whereby intruders can take advantage of the online system's database and manipulate votes. He said all this will compromise accuracy of votes and security of the system and its components.

“To add more on what my colleagues just said, network attack is one of the attacks related to online systems, database where voter's and votes information will be stored, can be easily

tempered with by intruders hence affecting election integrity, and security of the systems itself together with its availability which is supposed to be the core business of elections”
[Respondent 3]

“Confidentiality of voters will suffer as well, compared to the manual system whereby observers are tasked to look or guard the ballot boxes during voting and counting of votes”
[Respondent 4]

The study also found that respondents were also concerned about votes buying. They mentioned that Botswana, like other developing countries in Africa, has many low-income families, so such systems as online voting would present a greater opportunity for election candidates to practice vote buying normally known as voter coercion to fuel their interests by taking advantage of a voter’s family backgrounds. The proposed model solves coercion or vote buying by allowing voters to vote multiple times. This prevents coercion and vote buying as the coerced vote will be declared invalid immediately after another new ballot has been cast, only the last vote is being tallied. This method will also perform the entire tallying algorithm on encrypted votes. Homomorphic encryption will also be used to tally the votes first preferences. This will allow a single electoral authority who learns the contents of each vote, though the responsible authority does not learn the correspondence between voters and votes. This authority produces a transcript in which each step of the tallying process can be independently verified while revealing very little information, thus reducing the opportunities for coercion.

“Botswana like any other developing countries in Africa, most of the people are from low-income families, so such systems as online voting would present a greater opportunity for election candidates to practice vote buying or voter coercion to fuel their interests taking advantage of voter’s family backgrounds” [Respondent 5]

4.4 Cross Analysis of Responses

In this sub-section, the researcher cross-analysed responses from the survey and interviews based on respondent’s education level, computer experience of respondents, and confirm whether there is a positive relation between the variables and to determine whether

there is motivation and willingness to use a remote e-voting system if introduced in Botswana. The cross analysis method was used to identify any positive relationship among the identified variables. Results from this experiment were used in answering the research questions in this study.

1. In your opinion do you think the paper-based system has problems * Can e-voting reduce these problems

		In your opinion do you think paper-based system has problems?		Total
		Yes	No	
Can e-voting system reduce these problems?	Yes	180(97.3%)	5(2.7%)	185(100%)
	No	4(26.7%)	11(73.3%)	15(100%)
Total		184(92%)	16(8%)	200(100%)

Table 4.0.44- Correlation between paper-based vs. e-voting solutions

As can be seen from **table 4.0.41**, 180 (97.3%) of respondents agreed that the paper-based voting system has problems and they believe that remote e-voting system can reduce these problems. 185 respondents concurred that remote e-voting system would reduce these problems, and only 5 (2.7%) of respondents disagreed that paper-based voting system used in Botswana has problems.

2. Respondent's Educational background * Willingness to use E-voting system

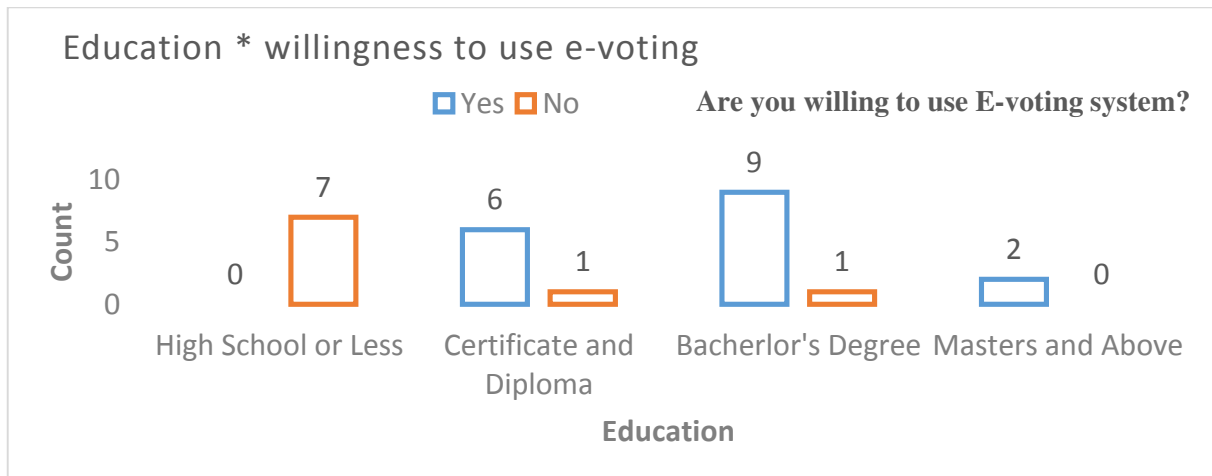


Figure 4.1 - Education vs. Willingness to use the remote e-voting system

According to **figure 4.1**, there is a strong link between educational level and willingness to use the remote e-voting system.

3. Reliability of the results of e-voting * Willingness to use E-voting system

This relation was done to check whether there is a relation between respondents willing to use e-voting system and whether they can rely on and trust the results of an e-voting system.

		Are you willing to use an e-voting system?		Total
		Yes	No	
Can you rely on the results of an e-voting system?	Yes	180(97.3)	5(2.7%)	185(100%)
	No	4(26.7%)	11(73.3%)	15(100%)
Total		184(92%)	16(8%)	200(100%)

Table 4.0.45- Reliability and Willingness to use an E-voting system

Table 4.0.45 shows the relation between reliability and respondents who are willing to use an e-voting system if introduced.

4 Respondent's computer experience * Type of voting technology preferred

The cross analysis was done to determine the relation between respondent's computer experiences and their preferred voting technology. **Figure 4.0.11** gives the illustration.

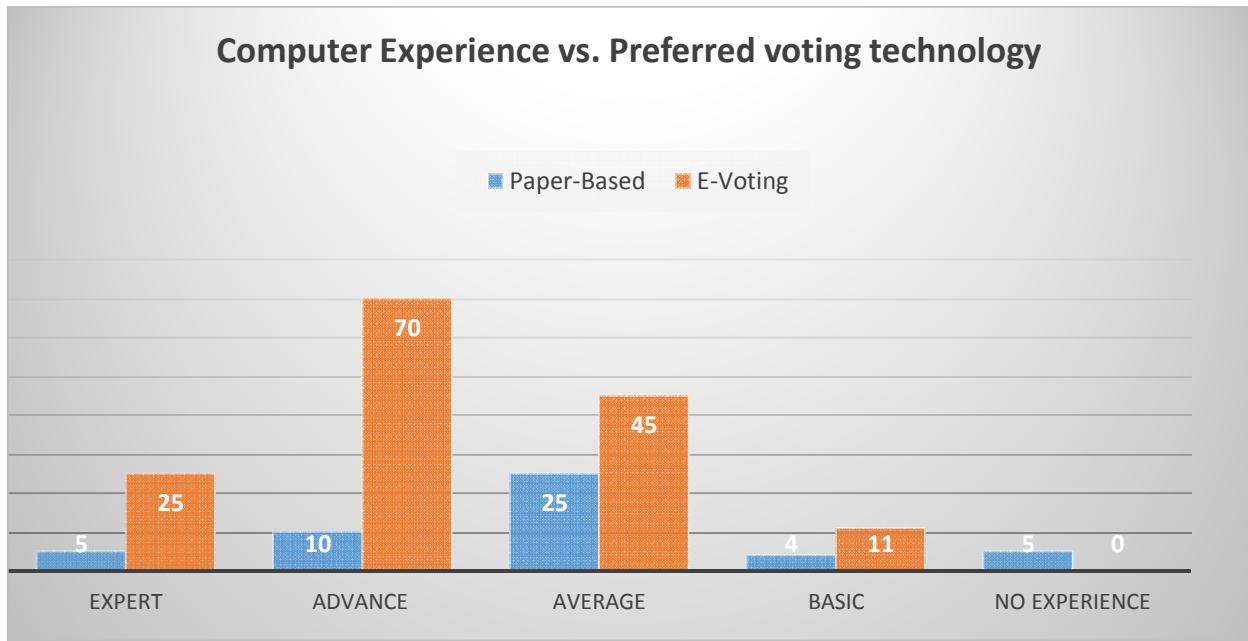


Figure 4.1 Computer experience and type of voting technology

Figure 4.2 shows the relation between respondent's computer experiences and the type of voting technology they are willing to use.

4.5 Conclusion

According to the findings, the current paper-based voting system has problems. These problems include, long queues, length of time taken by an individual to cast a vote, length of time for ballot counting, it is also expensive due to cost of hiring temporary poll stations officials. Respondents believed introduction of remote e-voting system is possible in Botswana in future. They expressed positive perceptions towards introduction of remote e-voting system and believed a remote e-voting system would bring positive changes and benefits to Botswana. The perceived benefits include, reduced chances of spoilt votes due to wrong markings, no manual counting which in turn eliminates the time taken for such an exercise and errors associated therewith, speeding-up the voting process, reducing long queues and the cost of running election would lower due to the requirement of less polling officers.

Although respondents expressed a positive attitude towards the introduction of a remote e-voting system, they also perceived it to have challenges. The challenges include the ICT infrastructure of IEC, possible attacks to the remote e-voting system either through the network, system server or voter interface as well as infringements like voter buying. The other challenge includes the high illiteracy rates among voters, and also lack of required ICT educational background among IEC employees.

Based on the perceptions and experiences of respondents, it is possible to introduce a remote e-voting system in Botswana. Voters and IEC employees need to be trained and educated on how to run and manage a remote e-voting system as they play an important role in introducing a new system. The identified variables were subjected to a cross analysis method to assess a positive correlation among them. The chapter below gives discussions of the findings.

CHAPTER 5

DISCUSSION

5.1 Introduction

This chapter presents discussion of the results of the four (4) objectives of this study and how they were achieved. This shall inform development of a conceptual voting model which can be used to develop and implement a secure remote e-voting system in developing countries.

5.2 Potential benefits of introducing remote e-voting in Botswana

The findings indicate that implementation of remote e-voting in Botswana is highly possible in future. The findings show that there will be several benefits of introducing and implementing remote e-voting system in Botswana, and the benefits shown by the survey include:

- ✓ E-voting would eliminate chances of multiple voting
- ✓ E-voting would reduce high number of spoilt votes
- ✓ E-voting would reduce long queues hence increase voting process speed
- ✓ Ballot counting would be fast, easy and reliable
- ✓ The respondents further perceived that introducing remote e-voting system would reduce costs for carrying elections as minimal number of election officers at polling station will reduce.

The study further indicates that voters preferred to use a remote e-voting system to cast votes compared to manual paper-based voting system. According to **table 4.0.42**, of 200 respondents, 95% opted to use a remote e-voting system, while only 5% preferred the traditional paper-based voting system. Further, studies carried out by Jambhulkaret *al*[5] shows that introducing remote electronic voting has a potential of restoring the democratic linkage between citizen's participation in elections, and consequently, restore the democratic linkage between citizens and political institutions. Studies by Adida [29] and Chaum *et al*[58]

further indicates that by introducing remote e-voting as replacement to traditional paper-based voting system will however influence young generation to partaking in elections as it is perceived to offer increased convenience compared to traditional paper-based voting system. It is believed to substantially reduce the costs of casting a vote. Based on the evidence confirmed by Geogiana *et al*[74], Kumar and Walia [11], with regards to time, evidence from Estonia shows that traditional paper-based voting is 16-times more time consuming than Internet voting. Literature further indicated that remote e-voting eliminates obstacles associated with bad weather, long queues, or confusion over location of polling places. Therefore, it has the potential of boosting turnout among the entire population as the voting process is made essentially more convenient. This supports findings from this study about potential benefits of introducing remote e-voting in Botswana which also gives answers to the first research question.

5.3 Security challenges hindering introduction of remote e-voting system in Botswana

This sub-section discusses the findings concerning security challenges hindering the implementation of remote e-voting system in Botswana. The responses were used to answer the research question (2) “*What are the security challenges that hinder the introduction and implementation of remote electronic voting in Botswana*”.

Findings have indicated that security challenges which hinders introduction of remote e-voting in developing countries Botswana included are: Security of ICT Infrastructure, client-side attacks, server-side attacks, Internet or network attacks and Vote Buying (*vote coercion*) [3][11][32][33].

5.3.1 Security of IEC ICT Infrastructure

According to *intervieweeNo2* from the third interview question, the current system in place consists of ICT infrastructure with little consideration of security architecture and standard requirements needed for a secure voting system. He further confirmed that the current ICT infrastructure was established without considering the current ICT security issues within the

field of voting, which is normally experienced by developed countries. Studies by Jefferson *et al* [90] and Olaniyi *et al*[75] further indicates that IEC infrastructure in developing countries are normally designed to support the manual paper-based voting systems where most of the workload is done manually. Therefore adopting remote e-voting system which is an ICT based voting system, will however requires the organization responsible for running election to purchase new set of ICT devices and a thorough training for IEC employees will be required. Therefore, introducing remote e-voting was perceived to be expensive and risky.

5.3.2 Client-Side Attack

The developed conceptual model requires voters touse their home computers or mobile phones connected via the Internet to cast their votes. Electronic devices such as phones and computers are vulnerable to attacks such as the one mentioned in *sub-section2.3.7* and theseattacks cannot be handled by the IEC officials alone, hence becoming too difficult to apply countermeasures at the client-side. The respondents were concerned that unreliable computers and mobile phones of voters will somehow create a serious problem which will lead to compromising the accuracy of the election results. Studies by Chaum [33] further indicates that common people are normally not concerned about the security of their computers, as some can go years without updating the anti-virus installed on their machines and this will also results in attacks from user machines used for voting.

According to [33][56][39], the possible attacks that can be caused by this malicious software (viruses) and the possible risks that could be encountered include:

- ✓ A malware may randomly alter a voter's choice without the user noticing. A computer affected with malware can easily cast a vote without the voter's consent.
- ✓ An attacker can also launch a denial of service (Dos) attack to the voter's machine to deny the voter a chance to cast their vote. **Figure 5.0.1** illustrates an attack launched against the voter.

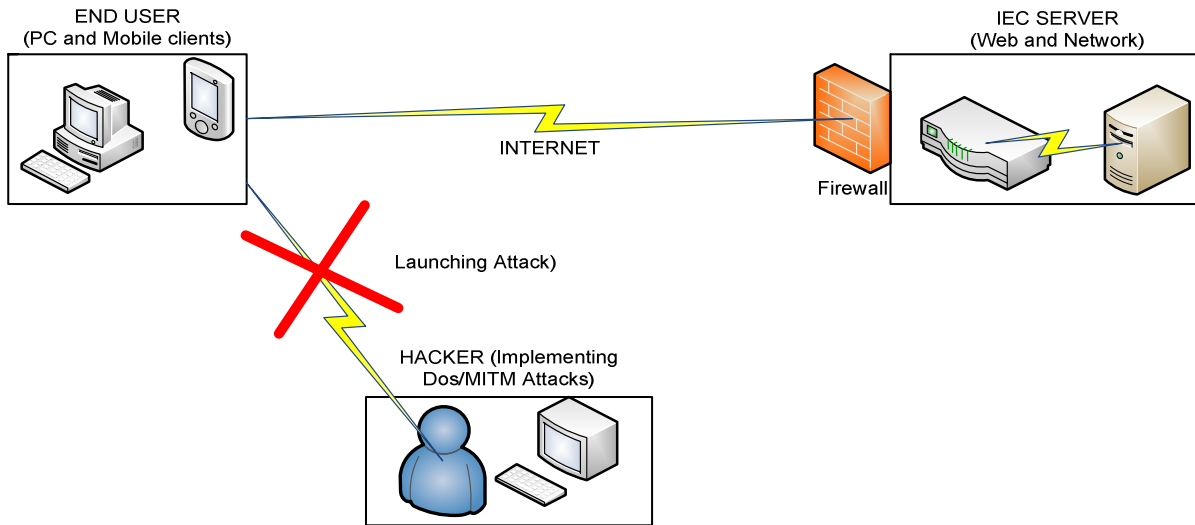


Figure 5.0.1 Client-Side attack

5.3.3 Server-Side Attack

The other attack experts were concerned about was a server-side attack. Interviewee No2, said that there would be a high possibility for intruders to take advantage of the online voting system by interacting with its interface or part thereof mainly to exploit vulnerabilities. Respondents further said this type of attack will compromise the accuracy of ballots, as well as the security of the system ultimately affecting the voting components or the system in its entirety. Some respondents raised fears of political malfeasance, stating that some political groups, especially those in the incumbent government would want to commit widely ranging fraudulent practices to protect their interests.

They also said there is a possibility of denial of service (Dos) whereby voters will be denied to vote. This attack is also known as *man-in-the-middle* attack (MITM). **Figure 5.0.2** gives an illustration of Server-Side attack.

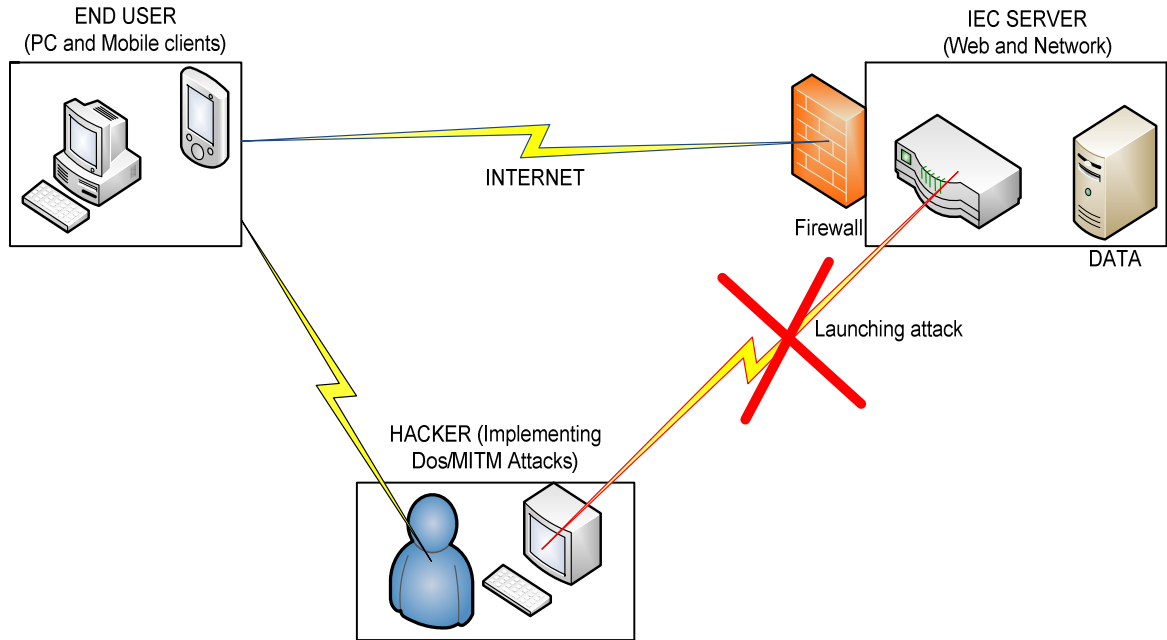


Figure 5.0.2 *Server-Side attack*

5.3.4 The Network or Internet Security Attack

Since the remote e-voting system will be transmitted over a network or the Internet, respondents were concerned that either the database containing the voter's information and ballots could be tampered with to the detriment of election integrity, and security of the system itself. Further to this the system's core business is to be fully available throughout the election period, and such tampering could impact negatively on its availability.

According to [20],[4],[40] other attack that is most probably to take place when a vote is transmitted over the Internet is spoofing. During a spoofing attack, an attacker can simply feed a voter with a similar and legitimate-appearing web page. When the voter casts their vote on such a page it would give the attacker a simple route into accessing and changing the voter's ballot as they will be having all the required information to cast a vote. Other network-based attacks include *TCP SYN attack*, *IP fragmentation* etc.[5],[52]. The **figure 5.0.3** illustrates an attack launched through the network.

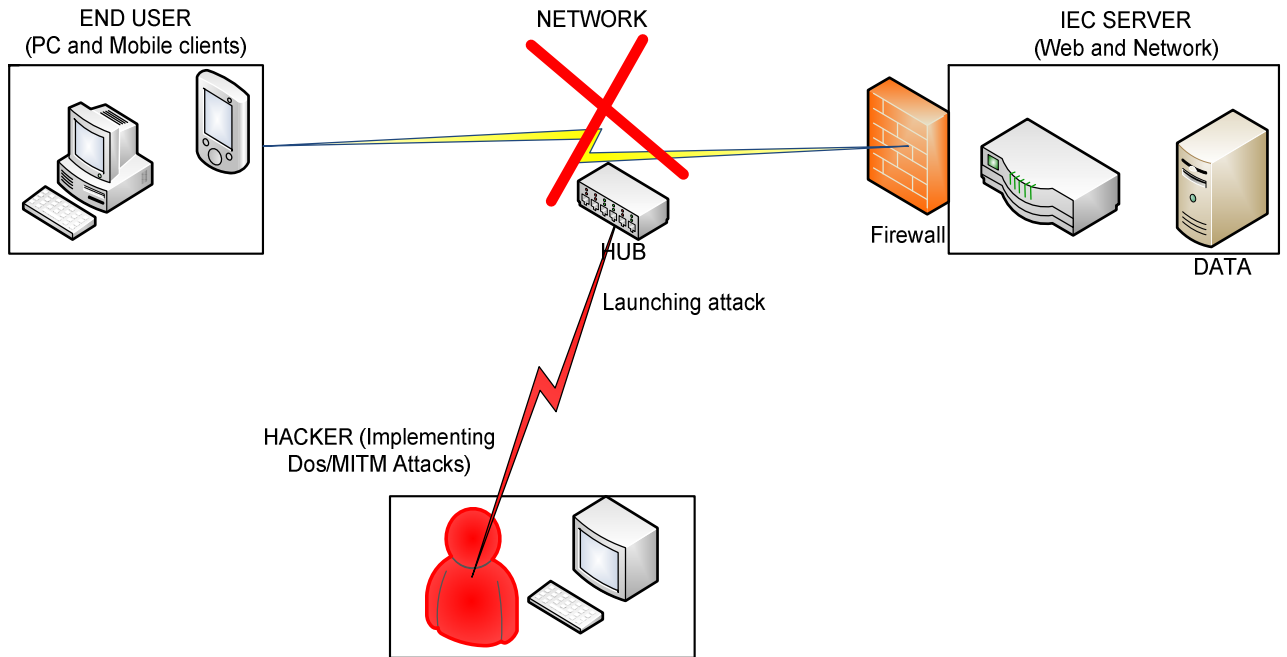


Figure 5.0.3 Network-Side attack

5.3.5 Vote Buying and Voter Coercion

The respondents were also concerned about the possibility of vote buying or voter coercion. Vote coercion is a situation whereby a voter is forced to cast his vote in a particular way[90]. Voter coercion is predominantly high in countries that are corruption-rife, poverty stricken and have high unemployment especially among youth. Such a phenomenon is not rampant in developed countries where the majority of voters are from rich or middle income families. The assumption is that in the case of Botswana an online voting system would present a greater opportunity for election candidates to practice voter coercion by taking advantage of a voter's family background.

5.4 Security Requirements

This sub-section gives the discussion on the identified security requirements for a secure remote e-voting systems.

5.4.1 Public Key Management

The function of this component is to ensure that the model voting approach provides an assurance towards fulfilling security requirements of electronic voting systems. This subsection describes the main concepts behind Public Key Management, main risks, and possible adopted controls. The proposed approach adopted RSA asymmetric cryptographic mechanism to ensure that secrecy and accuracy of tally results are achieved.

Under this mechanism, two different systematic key pairs are generated, the other one is public and the other is private. The public key is given out to all participating entities (Voter Application) and it is used for encrypting cast ballots. It is installed or integrated into voter's application. The private key is used to decrypt the votes. The other pair of keys belongs to the Voter's Application, the private key is used for signing the encrypted ballots (Enc_Bal) to generate signed encrypted ballots $Sign(Enc(v, r, PK), SK[i])$ before transference to the Back-Office for storage. And the public key is used by Votes Storing Server to compare signatures and check whether the signed encrypted ballot belongs to owners of the sessions.

In order to increase the secrecy of the developed voting model, only public keys are available to participating entities and private keys are not disclosed, and only used when necessary. They are only used during the signing of encrypted ballots Enc_Bal by Voter Application and when decrypting encrypted ballots Enc_Bal by offline Vote Counting Server. The Votes Counting Server of the developed model is made offline in order to prevent attacks from outsiders. The outside intruders can hack into the system online and maybe change the results in favor of other candidates, and compromising the accuracy of the election results and privacy of the voters.

When the election period ends, all the generated keys are destroyed and they cannot be used in the next elections. The main focus of the public key management is to ensure that all keys used within the election systems are secured and protected from outsiders (intruders). The secrecy of the electronic voting systems can be compromised in many ways, including the intruder having access to the private keys or having access to the digitally signed encrypted votes. When the intruders have access to the private keys and digitally signed ballots, they can do changes as they want, from changing voter's choice to altering election final results.

5.4.2 Identification, Authentication and Authorization Issues

The researcher adopted the double envelope method discussed in *sub-section 2.7* and the cryptographic digital signature scheme discussed in *sub-section 2.6.1* in order to ensure security, authenticity, and accuracy of the election results. According to this method, the vote is encrypted using the public key of the Votes Counting Server, while the corresponding private key remains hidden until the counting period. After the voter makes his final choice, he will then digitally sign the encrypted ballot Enc_Bal with his own private key $SK[i]$ to generate signed encrypted ballot $Sign(Enc(v, r, PK), SK[i])$ (outer envelope). After voting all the votes will be collected, sorted, and all the invalid votes will be eliminated from others as well as verifying eligible voters. Then the digital signatures (outer envelopes) will be separated from encrypted ballots (inner envelopes). The encrypted ballots together with the list of voters will be forwarded to the Votes Counting Server. The inner envelopes will no longer be linked or associated with the voters anymore, therefore no one will be able to know who voted for who. This helps to solve the problems of vote buying and selling as well bringing about secrecy and trust in using the online voting systems by respondents (voters). Voters are allowed to vote as many times as they want and only the last vote will be tallied.

The Vote Counting Server will then decrypt the encrypted ballots using the secured private key, and produce the final results of the elections. **Figure 5.0.4** depicts the double envelope method adopted by the developed conceptual voting model.

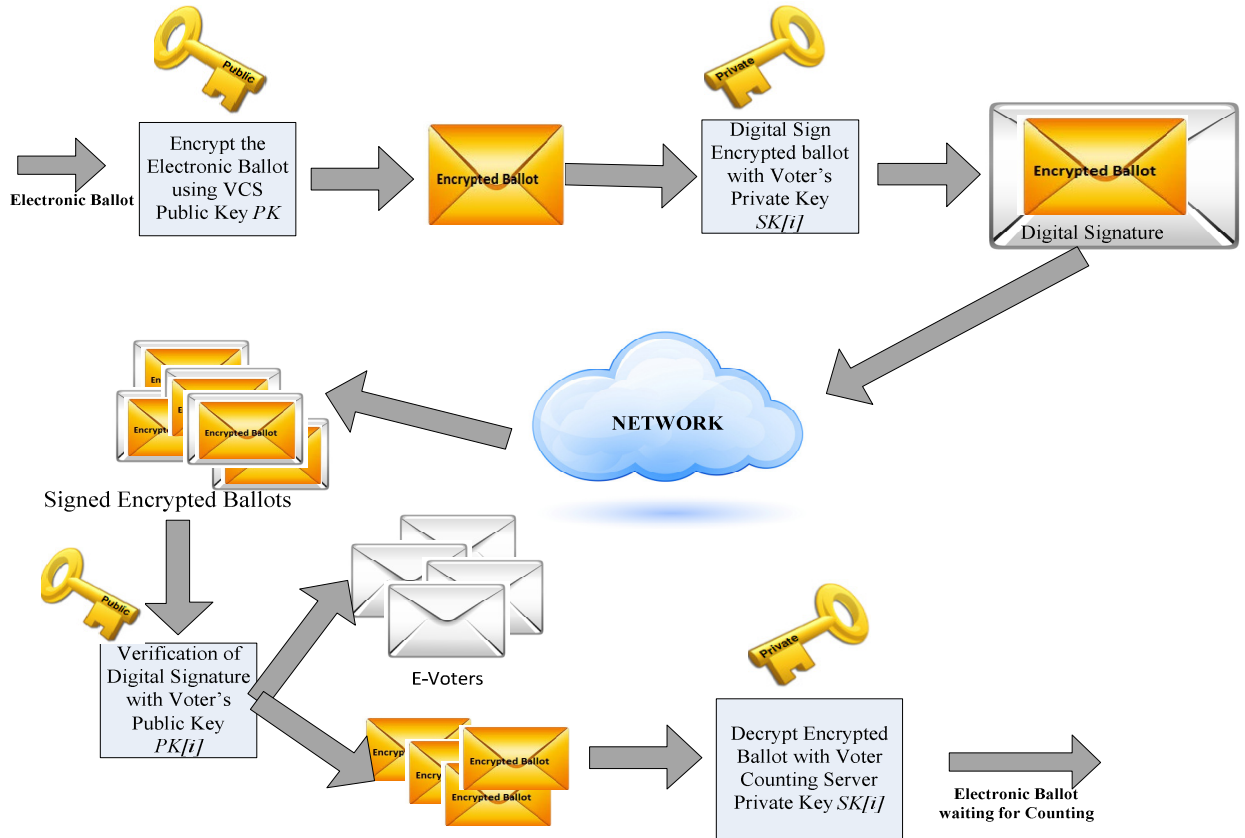


Figure 5.0.4 The double Envelope Method

The RSA digital signature scheme adopted for this developed model as discussed in **subsection 2.6.1** consists of three security factors, which includes message authentication, non-repudiation of the message, and data accuracy. The message authentication is used to assure the verifier (Votes Storing Server) when validating the digital signatures using voter's public keys $PK[i]$ that the digital signatures have been created only by the voters who possess the corresponding private keys $SK[i]$ not anyone else.

The data accuracy mechanism is used to track modification made to the signed encrypted ballots $Sign(Enc(v, r, PK), SK[i])$ when passed over the Network Server (Network) to the Back Office (Votes Storing Server) as demonstrated in the above **figure 5.0.5**. In the case when an attacker has access to the signed encrypted ballot, the digital signature verification at the receiver side (Votes Storing Server) will detect that change and notifies the sender (Vote Application) that the signed encrypted ballot has been modified. The hash value of the

modified ballot and the output displayed by the algorithm used for validation will not match. Therefore, the receiver (Vote Storing Server) can safely deny the received signed encrypted ballot assuming that ballot content integrity and accuracy has been breached. Therefore, the breached signed encrypted ballot will be thrown to a rejected list rather than sending it to a Vote Counting Server to wait for tallying and gives inaccurate results.

And lastly, the developed model uses *non-repudiation message mechanism* to bring about assurance of votes verifiability with the developed voting approach. When using this mechanism, it is automatically anticipated that only the person who signed the ballot has the knowledge of the signature key, so this gives voters an opportunity to create a unique signature on a given data. Hence, the receiver (Vote Storing Server) can present the encrypted ballot data together with the digital signature to someone else as proof if any dispute arises in the future. So with the developed voting approach, when the voter wants to confirm that their vote has been *recorded-as-cast* or *tallied-as-recorded* the Back-Office (or Election Officers) can easily provide the evidence to the concerned voter.

Basically, to ensure authenticity, secrecy, and accuracy of election results, the researcher combined RSA public-key encryption with the digital signature scheme as discussed above in order to create a cryptosystem that can provide the four essential elements of security namely: Privacy, authentication, accuracy, and non-repudiation. The combination of the two mechanisms helped the researcher to meet his aim of developing a conceptual model which can be used for designing and implementing secure and trusted online voting systems.

5.4.3 Addressing Vote Buying and Coercion Problems

The respondents raised concerns about vote buying if remote e-voting would be introduced. In a remote e-voting system, candidates can coerce voters easily without being caught. So to reduce the impact and negative consequences associated with this issue, the researcher adopted the vote-more-than once scheme used by the Estonian Voting Model.

This scheme allows voters to vote more than once, and only the last vote will be considered and the rest will be canceled from the Votes Storing Server. This option gives voters an opportunity to vote as they want because potential buyers will never know which vote will be counted in the final tally.

5.4.4 Ensuring Vote Verification

To ensure vote verification within the developed conceptual model, the researcher introduced *non-repudiation message mechanisms* discussed above in *sub-section 2.6.2*. This indicates that each registered voter can verify that his vote has been counted correctly in the final tally by using published data. The model allows auditing using published data, and all the processes involved in the voting system have to be audited. This can be made possible by using vote verification code from vote receipt generated at the end of voting. These codes are sent directly to voters through vote application interface. After receiving the feedback, voters can now compare between their selected options and receipt codes. If the receipt code matches their selections, voters could now be assured that their votes are *recorded-as-cast* and *tallied-as-recorded*.

5.4.5 Addressing Man-In-The-Middle (MITM) and Denial of Service (Dos) attacks

According to the literature[90], it is difficult to prevent such attacks, however, they are easy to be detected. Denial of service attack is one type of cyber-attack that mainly focuses on disrupting the availability of services. There are mechanisms that can help to reduce the impact of an attack when it occurs. This includes an adaptation of a very strong risks mitigation plan that could help to avert the occurrence of DOS in electronic voting systems.

This attack varies from physical IT environment destruction to make use of the system's flaws and overload the network capacity. To reduce the issue of DOS, the study makes an assumption that DOS attacks based on local malware can only affect a minimal number of voters from voting. The developed model uses distributed servers which will lead to a higher availability, unlike in a centralized server which relies in a single data center which will make the system to be vulnerable to attacks such as DOS or similar attacks. The approach also uses a robust disaster recovery plan to avert the impact associated with DOS attacks.

5.5 Conceptual Model

This sub-section covers the development of the conceptual model, which was designed through data from desk review technique and results from study findings. The researcher reviewed different existing voting models, and system to identify their weaknesses and strengths. The security requirements for secure remote e-voting system are identified, as well as responses from the survey and interview responses, were both taken into consideration when developing the conceptual model.

The developed model was designed as a merging of two models, the Estonian voting model, and Norwegian voting model. This approach consists of a number of additional features which distinguishes it from both the Norwegian and Estonian models. The features are as follows:

- ✓ Implementation of Public Key Infrastructure (PKI), together with the use of Voter Identification Number (Student ID #) and Voter confirmation code which is generated during registration. The authentication of online voting and voter's digital signature are applied by using PKI. This combination is used for voter identification and authentication.
- ✓ The use of RSA digital Signature for signing the encrypted votes and voter's login details.
- ✓ The use of confirmation code which is normally used to bring about transparency while maintaining vote secrecy.
- ✓ It also includes a registration phase, where all voters are requested to register before taking part in elections.

Other generic and key principles to which the approach is required to comply with in order to meet required basic requirements for secure online voting systems include,

- ✓ *Privacy*: After voting, no one should be able to link the voter to their vote
- ✓ *Authenticity*: Authenticity refers to one-voter-one-vote rule

- ✓ *Integrity (Accuracy)*: Once a vote is cast, no one should be able to modify or delete that particular vote. All valid votes should be included in the final tally and all invalid votes should be discarded.
- ✓ *Security*: Throughout voting, all votes should not be tempered with.
- ✓ *Democracy*: All eligible voters should be given equal chance to cast their votes, the one-person one-vote rule must apply, and no one should be allowed to vote more than once or vote for others.
- ✓ *Verifiability*: Voters should be able to verify on their own that their votes have been counted correctly and included in the final tally.
- ✓ *Multi-Users*: The model should allow multiple users to cast simultaneously without any problems.
- ✓ *Accessibility*: The system should allow voters to access it from any geographical location using their computers or mobile phones.
- ✓ *Availability*: The system must be available throughout the elections.

5.5.1 Conceptual Model Architecture

The developed architecture has been designed by taking into consideration the geographical location, size, environment, infrastructure and population density of Botswana. The architecture is divided into three main sections. *Figure 5.0.5* illustrates the developed conceptual architecture.

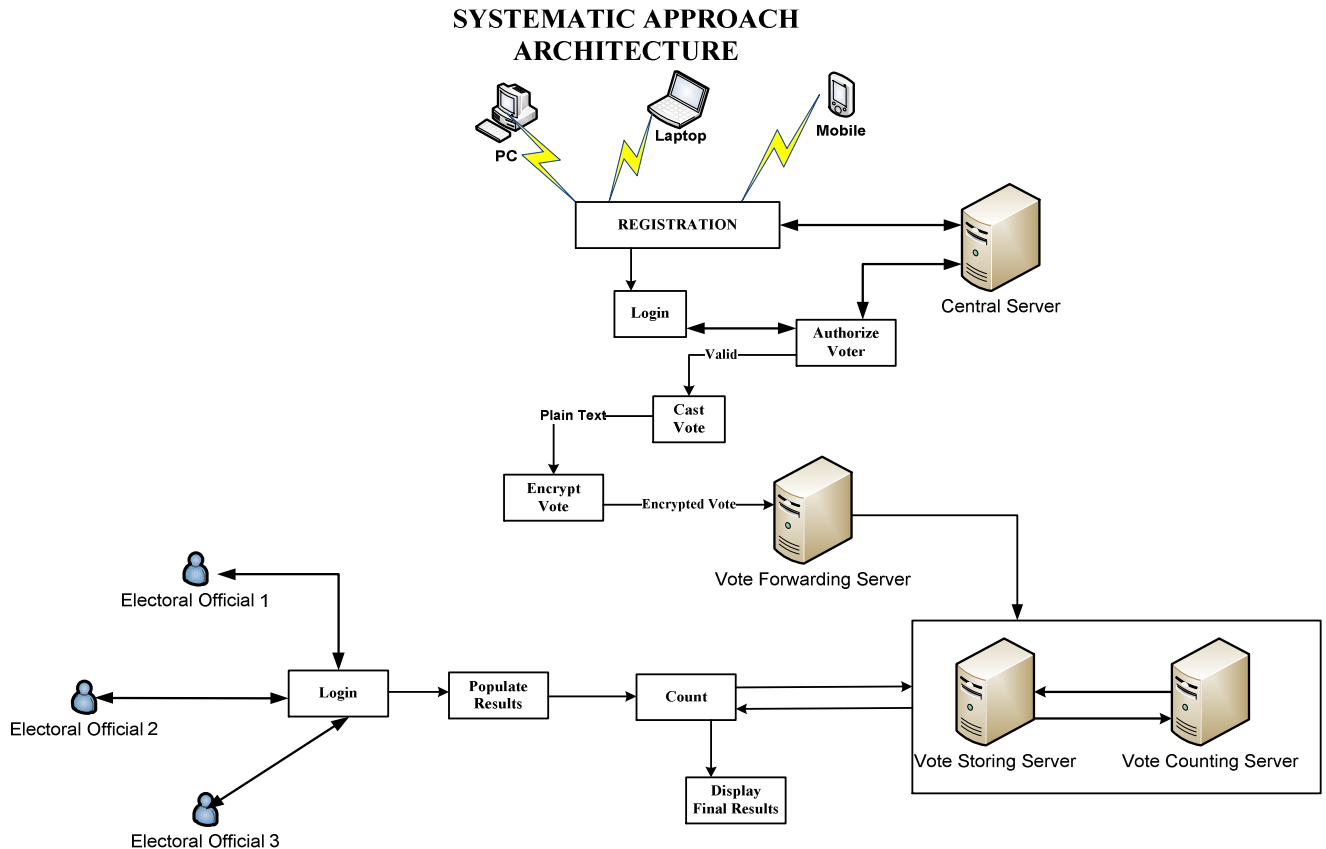


Figure 5.0.5 *Conceptual Model Architecture*

Pre – Voting Phase

a. Registration process

The registration process involves voters registered into the voter's roll and provided with security credential which will be used to verify their identity when they login into the system or authorize access when casting votes. The credentials include a login password, username and the voter confirmation code which is generated through the use of Public Key Infrastructure (PKI).

All voters are provided with Identification Cards (ID cards) by the registry departments when enrolling with the IEC, so their National Identity Card Numbers will be used to identify and authenticate voters. The security credentials should involve the three-factor authentication mechanism to identify and authenticate all eligible voters. The three-factor authentication mechanism includes the voter's ID cards, digital certificates, and confirmation code.

Voting Phase

b. Voting process

The voting process involves authentication and identification of voters, vote casting, encryption and signing of votes, votes recording and storing by the backend servers, even verification of votes. In this phase, eligible voters cast their votes and the system saves all valid votes into the Voting Storing Server before sent to Voting Counting Server where the final results are published. The process is explained in details in *sub-section 5.3.2*.

Post-Voting Phase

c. Counting and Results display

This is the phase where valid votes are sorted and managed, then decrypted and counted followed by the publication of final results. The votes auditing process also falls under this phase. This process checks whether eligible voters were capable of casting votes and if their votes were included in the final tally.

5.5.2 Conceptual Model Infrastructure

The developed voting model is divided into three main components of infrastructure:

- ✓ Voter's applications (*e.g. web application*)
- ✓ Network Server
- ✓ And Back office (*consists of Vote Storing Server (VSS) and Vote Counting Server (VCS)*)

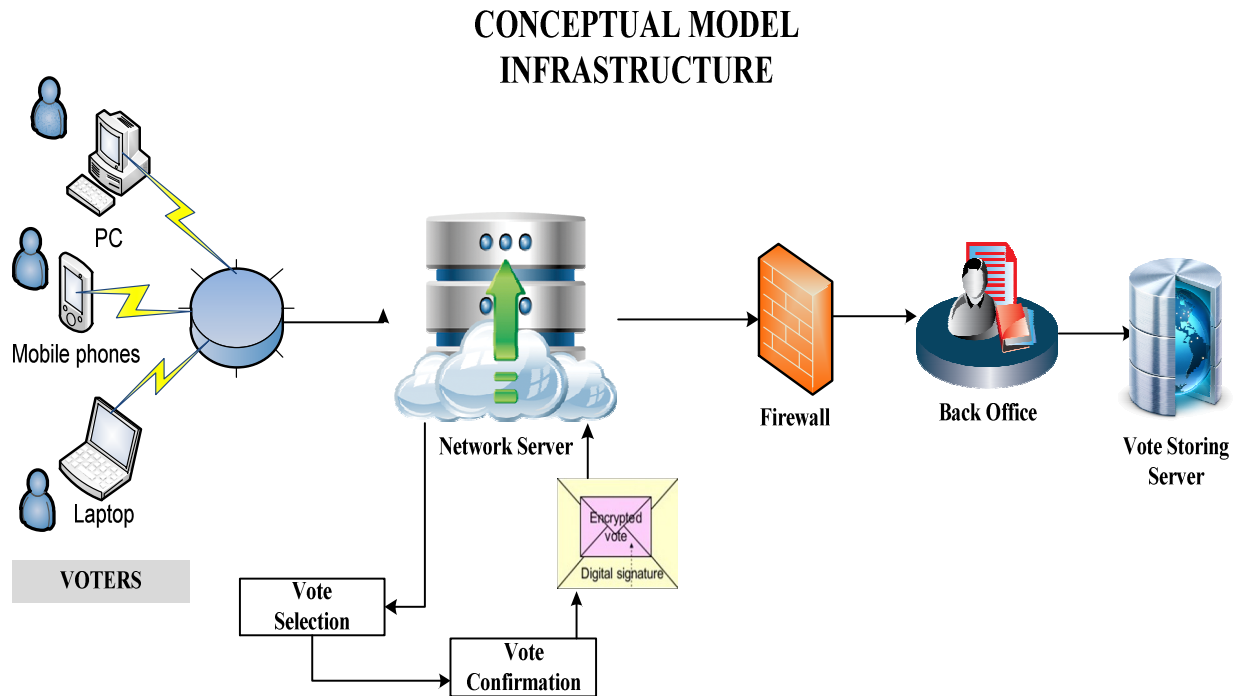


Figure 5.0.6 *Conceptual Model Infrastructure Components*

A. Voter Application

This is a web-based application located at the client-side. It is normally installed inside voter's computers or electronic devices or accessed through the use of voter's voting devices. The voter's application connects to the Network Server in order to allow or create communication between the client-side and the server-side (back office servers). The encryption and authentication process is built into the Secure Socket Layer (SSL) protocol to ensure that communication between Clients Server (CS) and Network Server (NS) is secured. This helps to monitor and block access to ineligible voters from voting.

B. Network Server

This is an online based - server that supplies voters with a necessary platform for casting their votes. It creates a connection between client-side and back-office servers to transmit encrypted signed votes for storage and counting. The Network Server performs confirmation of voters through user authentication process and releases the list of registered candidates. After the voters have cast their votes and confirm their selections, the cast votes will be encrypted using the public key *PK* of the *Vote Count Server (VCS)* and signed using the

voter's personal private key $SK[i]$ to generate a signed encrypted ballot $Sign(Enc(v, r, PK), SK[i])$. The signed encrypted ballot will then be transmitted through Local Area Network (LAN) to the Back-Office. The votes at the back-office will then be transferred to the *Vote Storage Server (VSS)*.

Generally, the purpose of this server is to authenticate a voter's personal information, to send a list of candidates, to authentic voters and also receive cast votes which have been encrypted with the public key PK of the Vote Counting Server and signed with voter's private keys $SK[i]$ before forwarding the encrypted and signed votes $Sign(Enc(v, r, PK), SK[i])$ to the Back-Office.

C. Back Office

The back office consists of a number of servers which serves different purposes, from storing and maintaining votes, and to counting votes and publishing of final tally. The Back office receives the signed and encrypted votes from the network server and transfers them to the Vote Storing Server (VSS) to ensure that only eligible voters cast votes and also to maintain the accuracy of the results. The back office checks the signatures of the ballots and verifies whether the voters had already voted before and whether any modification took place during transmission of votes through the network or the Internet.

When the election period elapses, the Vote- Storing Server sends the valid votes to the Vote-Counting Server (VCS) to execute final tally and publish the final results. The VCS uses its private key (PK) to decrypt the votes.

Vote Storing Server (VSS)

The main purpose of this server is to store and eliminate the invalid votes by comparing the signatures of the votes (outer envelopes) to check whether any modifications were made during transmission of votes from Client and Network Servers. The rejected votes will be stored into a reject list log before sending an acknowledgment to voters informing them of the action taken. This server is also responsible for separating encrypted ballots from voter's signature and also verify if the particular voter or the owner of the signed encrypted vote is eligible to vote.

Vote Counting Server (VCS)

The main function of this server is to decrypt cast votes using its own private key SK . The public key PK of this server is used by all voters when encrypting their cast votes. This vote is being encrypted with election's public key, signed with the voter's private key (*double envelope*, see 2.5) and sent to the Vote Forwarding Server, which forwards the correctly encrypted ballot to the Vote Storage Server and leaves a log entry on a special Log Server. These three servers are deployed in a data center controlled by the election authorities. Before sending the encrypted ballot to the Vote Counting Server, voters are allowed to vote multiple times to prevent coercion and vote buying. The encryption, decryption and digital signature mathematical theorem for the used algorithm (RSA) is as follow.

Encryption

- *Vote Storing server obtains Voters' List server's authentic public key (n, e) , where e is the encryption exponent and n is the modulus.*
- *Vote Storing server represents the voter's details as an integer m in the interval $[0, n - 1]$.*
- *It then computes $c = m^e \mod n$.*
- *And send the ciphertext c to the Voters' List server.*

Decryption

- *The Voters' List server uses its private key d to recover $m = c^d \mod n$*

Digital Signature

The voting server uses the RSA algorithm for signing the votes. The signing process is presented as follows: the Voting server has a public key (n, e) and private key d . b is the ballot of the be signed, and k is a random number between 1 and n .

- *The Voting server computes $b = k(b)$, an integer in the interval $[0, n - 1]$.*
- *It then computes $s = b^d \mod n$.*
- *The signature of the Voting server is s .*

The Vote Storing server verifies the Voting server's signature s and recovers the ballot b using the following steps:

- *It obtains the Voting server's public key (n, e) .*
- *It then computes $b = s^e \bmod n$*
- *And lastly computes $b = k^{-1}(b)$.*

5.5.3 Conceptual Model Voting Process

The developed conceptual model requires that the process of voting or casting votes start first with voters being issued cards (voter's identification cards). The card should contain all the necessary information for the voter together with the pre-computed randomly and uniquely generated numbers (codes) corresponding to possible voting options on the election ballots. The proposed voting process is as follow:

- ✓ Firstly voters are allowed to go through registration to create their login credentials because the proposed approach uses password-based authentication and voter registration process. A unique key or PIN is given to each voter during registration, and after registration the voter's information will be sent to the database.
- ✓ During the Election Day, the voter launches the voter application by connecting via the *HTTP* protocol to the Network Server and supplies their login credentials (passwords and the uniquely generated number r) together with the Voter ID number (VID) to establish Secure Socket Layer (SSL) connection to authenticate them.
- ✓ The Network Server verifies the voter's franchise by sending a query to IEC registry database to check whether the particular voter exists on their database. If the voter does not exist, an error message will be sent to the Voter's application. In the case of positive results, the Network Server sends another query to the Vote Storing Server to check whether the voter has already voted before. If the results are positive, a connection will be established. And once the connection is established, the Network Server will forward the list of eligible candidates to the Voter Application for voters to make their choices.
- ✓ Next, the Voter's Application generates a random number r which helps to ensure non-deterministic cryptogram and encrypts the vote together with the randomly

generated number through the use of the RSA public key of Vote Counting Server to produce a ciphertext $Enc_bal = Enc(v, r, PK)$, which is called an encrypted ballot.

- ✓ The voter then signs the encrypted ballot by using his own private key $SK[i]$. The Voter Application will then forward the encrypted and signed vote $Sign_Enc_Bal = Sign(Enc_Bal, SK[i])$ to Network Server.
- ✓ The Network Server checks whether the session owner is the one who signed the encrypted ballot. And in the case of the positive results, the Network Server will then pass the signed encrypted ballot to the Back-Office (Vote Storing Server). If the results are negative, the Network Server will send an error message to Voter Application.
- ✓ The Vote Storing Server receives and stores the signed and encrypted ballots before passing them to the Vote Counting Server. This server confirms the signatures of each ballot and checks whether received ballot's signatures corresponds to the original voter's signatures. If there is no match, or if any changes were applied to the ballot content during transmission the Vote Storing Server will eliminate that particular ballot from other valid ballots, and send a message to the owner of the ballot to cast his ballot again. This server helps to ensure that only valid votes are passed through to the Counting Server and this helps to produce accurate and trustworthy election results.
- ✓ The Vote Storing Server then separates the encrypted ballots Enc_Bal (inner envelopes) from voter's personal signatures (outer envelopes), and then forward the encrypted valid ballots together with the list of voters to the offline Vote Counting Server through the use of data carriers.
- ✓ Then the Vote Counting Server performs decryption of valid votes using its own private key $SK[i]$ and then verifies if the format of the decrypted ballots corresponds to the fixed rules. All the invalid encrypted votes are stored inside the reject list because the Votes Counting Server counts only the positively verified votes and produces the results which are later published at the end of the election.

Data Item	Explanation
PK	The public key used to encrypt the cast ballot
SK	The private (secret) key used to decrypt the encrypted ballots
SK[i]	The private signature key for all the eligible voters
PK[i]	The public signature key for all the eligible voters
<i>v</i>	A voter's choice (ballot)
<i>r</i>	A randomly generate unique number
<i>bal</i>	A ballot generated from the combination of the voter's choice <i>v</i> and a random number <i>r</i>
<i>Enc_Bal</i>	Encrypted Ballot
<i>Sign_Enc_Bal</i>	Signed Encrypted Ballot
<i>VID</i>	Voter Identification Number

Table 5.0.1 Data items and explanations

5.6 Conclusion

The research findings indicate that it is possible to introduce and implement remote e-voting in Botswana in the future in spite of the misgivings expressed by some of the respondents regarding the current IEC infrastructure and educational level of IEC staff. The respondents stated that IEC infrastructure requires upgrading to cater for new voting technology, and that IEC staff would need to be resourced on how to operate and maintain the said technology at optimum efficiency. They further stated that voters, especially from rural areas would require training on how to use remote e-voting.

The discussion and results of the findings lead to the development of the conceptual voting model. The focus of this model is centered on modern cryptographic techniques aimed at securing information and data across different platforms which involve the use of user's personal information as it is transferred from one point to another over the Internet. The reviewed literature indicated that cryptographic technologies are the right tool to address these issues.

The developed voting model offers an assurance that the discussed voting information security issues hindering introduction and implementation of remote e-voting in Botswana will be addressed effectively and adequately. The approach consists of trustworthiness, confidentiality, integrity, data authentication, together with information security and accuracy which are required as the target issues for the developed model. The model is the upgrade of the two adopted models discussed in section 2 (*sub-section 2.2.1.1 and sub-section 2.2.1.4*). The conceptual model uses cryptographic technology for authentication, verification and encryption/decryption of voting information. It is also based on existing literature in mainstream electronic voting data security, accuracy, and data privacy relevant for understanding electronic voting system's security challenges.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

The chapter covers the conclusion of the study carried out and recommendations that needs to be considered by the IEC officials when introducing remote electronic voting system as well as limitations faced by the researcher to fully achieve the general objective of the study, followed by further studies to be carried out in order to fill the missing gaps.

6.2 Conclusion

The study found that manual paper-based system experiences poor voter turnout during elections due to the problems and challenges they face when using the system. These challenges include the time taken when voting, due to manual counting of votes, long queues, high number of spoilt votes, and cost of carrying elections. Voters felt it is not appropriate for people who are always busy (*students, and employees*). Others said voting normally takes place during working hours hence hindering them from attending elections while others feel that the system in place is old fashioned.

Other challenges discovered during this study include security challenges from a technical perspective that hinder the introduction and implementation of remote electronic voting in developing countries. These challenges include the high rate of illiteracy among the voting population and a shortage of electricity supply in rural areas, and a lack of ICT infrastructure that supports implementation and management of a remote e-voting system. They further stated the low level of skill manpower among IEC staff. Therefore, more training and education will be needed to set them ready to adopt, operate and manage the implementation of the new voting system within their organization.

The study also revealed that IEC staff belief that if e-voting is adopted and implemented in Botswana it will bring several benefits to IEC organization. These benefits include, reduced

operating cost of running election as less number of staff at polling stations will be required, e-voting will speed-up voting process and produce reliable results, it will also reduce voting fraud, and they also said it will reduce chances of counting errors and delays in publishing the results.

The undertaken study also identified security requirements that should be followed when designing or implementing remote electronic voting systems. These requirements are in line with general principles of democratic and peaceful elections.

The researcher reviewed and analyzed a number of similar remote electronic voting systems and models with respect to security and accuracy. Two similar models (*Estonian and Norwegian models*) were adopted and enhanced to develop a secure conceptual model which can be used to design and implement remote electronic voting systems. A thorough conceptual demonstration was designed which shows how this conceptual model, if well implemented can rectify the identified security challenges and fulfill the given general principles of democratic elections. The conceptual model was developed using desk review technique as explained above together with the engagement of security experts in the field of voting, and the feedback from the survey.

According to security experts and study findings, limited consultations were made when designing Botswana IEC Voting System ICT Infrastructures on how data collected from voters and votes needs to be stored or secured in order to satisfy security requirements for remote electronic voting systems. Therefore, from a technical perspective, it clearly shows that the ICT infrastructure was developed without any consideration of existing security issues. The computers and other network devices used by the IEC does not provide enough level of security with respect to authentication, authorization, and securing of voters and poll information.

Based on the findings, the ICT infrastructure adopted by the electoral committee of Botswana has a room for improvement to enable secure elections through the use of remote electronic voting system. This led to the proposal of a conceptual model for designing and implementing of secure e-voting systems with emphasis on security and results veracity.

6.3 Recommendations

The following recommendations are proposed to address challenges and problems faced when using the traditional paper-based voting system in Botswana. The recommendations are based on the voters' experiences in using the system and challenges faced by IEC officials and security experts in administering the manual paper-based system used in Botswana.

According to the study carried out, for a remote electronic voting system to be successful, it must ensure that all the security requirements and proper controls discussed in chapter 2 are implemented. The current ICT infrastructure and information security landscape adopted by Botswana IEC does not guarantee this level of security and accuracy. Therefore, this study recommends that:

- ✓ The remote electronic voting system should be equipped with a voter verification paper trail, which would eliminate many of the possible attacks.
- ✓ The voting system must ensure the reliability, usability, security, and verifiability of public elections is fundamental to a stable democracy. It should also have validation and verification processes to assure the security and reliability of the remote e-voting protocols and systems.
- ✓ There should also be well documentation and feedback on all the election processes to prevent the mistakes happened and to improve the process for next election.
- ✓ The proposed conceptual voting model to be used as a starting point for a long term strategic plan and objective to introducing the remote electronic voting system in Botswana. Introducing remote electronic voting system, may rekindle populace interest in elections, hence boosting voter turnout.
- ✓ And before election, poll workers and voters must be given a thorough training to reduce mistakes that might arise during elections.

The study also further recommends that IEC not immediately implement remote electronic voting, but to rather carry out a number of pilot and test projects. According to the study conducted, it shows that for a remote electronic voting system to be a success, professional and proper pilot studies need to be carried out in order to capture voter's opinions and perceptions on the particular system.

6.4 Limitations

To conclude the dissertation, there is a need to reflect on the general limitations that have been highlighted at given points of the work and identify areas for future research.

- ✓ The first limitation relates to the approach used when collecting data for this research. The researcher decided to opt for the cheaper and fast way of collecting research data, which is a mixed method.
- ✓ The second limitation this research faced was the difficulty to arrange a meeting for an interview with the expert personnel, it took long time to fulfil the survey procedure as IEC experts were engaged with other commitments.
- ✓ The other limitation is aligned with the sample size used. The study is limited to one setting and has a small sample size. Most of the empirical study relied on data collected from BIUST undergraduate's students and IEC election experts without covering other security professionals and lawmakers within the area under study.

Still, however, the research would have benefited enormously from other security professionals, both non-technical and technical, more especially to validate and confirm some of the emerging issues concerning voting in Botswana. Respondents could also have given useful insights on their exact knowledge on user requirements that would feed into the design and evaluation processes of the developed model. At the same time, it is highly acknowledged that prototyping would have been the best way to validate the model, but rather expert evaluation has been performed instead, and this is due to lack of resources and limited time frame. However, future work could focus on this area and maybe attempt to implement the model.

6.5 Further Research

Further research in the area of voting is recommended in the developing countries. Due to time constraints and funding, the study was limited to a small sample size comprising university students and security professionals. There are other cryptographic mechanisms that can be adopted and enhanced to boost perceptions and beliefs of voters on using remote electronic voting systems.

Further research is recommended to explore the experiences and perceptions of security professionals within the field of voting because the results of this study are still uncertain and need further improvement and justifications because the characteristics of the developed conceptual model defined are arguable. It is therefore very urgent and necessary to continue conducting a further study about society characteristics and the creation of more realistic environment models which will somehow promote the use of remote electronic voting systems in developing countries. So we believe that the results of this research can be extended for a remote electronic voting scenario and attempt to implement the developed model.

REFERENCES

- [1] R. Mercuri, "A Better Ballot Box?," *IEEE Spectrum*, vol. 39, no. 10, 2002, pp. 46-50.
- [2] R. Jardi-Cedo, J. Pujol-Ahullo, J. Castella-Roca and A. Viejo, "Study on poll-site voting and verification systems," *ELSEVIER - Computers and Security*, 2012, pp. 989-1010.
- [3] V. Mateu , F. Sebe and M. Valls, "Constructing Credential-Based E-Voting Systems from Offline," *Journal of Network and Computer Applications*, 2014, pp. 39-44.
- [4] S. Canard, M. Gaud and J. Traore, "Defeating malicious servers in a blind signatures based voting system," in *Proceedings of Financial Cryptography (FC'06)*, 2006, pp. 122-145.
- [5] S. M. Jambhulkar, J. B. Chakole and P. R. Pardhi, "A Secure Approach for Web Based Internet Voting System using Multiple Encryption," in *International Conference on Electronic Systems, Signal Processing and Computing Technologies*, India, 2014, pp. 12-34.
- [6] S. Lokhande, D. Sawant, N. Sayyad and M. Yengul, "E-Voting through Biometrics and Cryptography-Steganography Technique with conjunction of GSM Modem," in *Emerging Trends in Computer Science and Information Technology -(ETCSIT2012) - Conference*, India, 2012, pp. 101-134.
- [7] D. Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," *IEEE Security & Privacy*, vol. II, no. 1, 2004, p. 38–47.
- [8] T. Afrin and K. J. Satao, "Detailed Implementation of E-Voting System for on Duty Persons using RSA Algorithm with Kerberos Concept," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 7, 2013, pp. 1501.
- [9] A. I. Ali, "Comparison and Evaluation of Digital Signature Schemes employed in NDN Network," *International Journal of Embedded systems and Applications(IJESA) Vol.5*, 2015, pp. 15-29.
- [10] H. Brink, *Fundamentals of research methodology for health professionals*, Cape Town: Juta and Co (Ltd), 2006.
- [11] S. Kumar and E. Walia, "Analysis of Electronic Voting system in Various Countries," *International Journal on Computer Science and Engineering*, vol. III, no. 5, 2011, pp. 1825-1830.
- [12] B. Adida, "Helios: Web-based open-audit voting," in *In Proceedings of the Seventeenth Usenix Security Symposium (USENIX Security 2008)*, 2008, pp. 10-16.
- [13] C. Bull, "Countries with E-Voting projects," 3 December 2010. [Online]. Available: <http://aceproject.org/ace-en/focus/e-voting/countries> [Accessed: 12/10/2016].
- [14] E. R. Arnold, *History of Voting Systems in California*, Secretary of States, 1999.
- [15] M. R. Alvarez, T. E. Hall and A. H. Trechsel, "Internet Voting in Comparative Perspective: The Case of Estonia," *Political Science & Politics*, 2009, pp. 497-505.
- [16] B. Adida, "Helios: Web-based Open-Audit Voting," Harvard University, 2008.

- [17] O. Baudron, P. A. Fouque, D. Pointcheval, J. Stern and G. Poupard, "Practical multi-candidate election system," in *Proceedings of the 20th ACM Symposium on Principles of Distributed Computing (PODC'01)*, New York, 2001, pp. 201-214.
- [18] R. Jardi-Cedo, J. Pujol-Ahullo, J. Castella-Roca and A. Viejo, "Study on poll-site voting and verification systems," *ELSEVIER - Computers and Security*, pp. 989-1010, 2012.
- [19] CGI Group Inc, "Public Key Encryption and Digital Signature: How do they work?," *Business solutions through information technology*, 2004.
- [20] A. I. Ali, "Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network," *International Journal of Embedded systems and Applications(IJESA) Vol.5*, 2015, pp. 15-29.
- [21] M. J. M. Chowdhury, "Comparison of e-Voting Schemes: Estonian and Norwegian Solutions," *International Journal of Applied Information Systems (IJ AIS)*, 2013, pp. 60-66.
- [22] D. E. Denning, "Digital Signatures with RSA and Other Public-Key Cryptosystems," *Communications of the ACM*, New York, 1984.
- [23] A. Neff, "Practical High Certainty Intent Verification for Encrypted Votes," Montreal, Canada 2004.
- [24] J. Cohen and M. Fisher, "A Robust and Verifiable Cryptographically," in *Proceedings of the 26th IEEE symposium on the Foundations of Computer Science (FOCS'85)*, 1985, pp. 75-94.
- [25] A. Shamir, R. L. Rivest and L. M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," in *Communications of the ACM*, 1978, pp. 120-126.
- [26] T. ElGamal, "A Public Key Cryptosystem and A signature Scheme Based on Discrete Logarithm Problem," *IEEE Trans. Info. Theory*, 1985, pp. 469-472.
- [27] S. Katiyar, K. R. Meka, F. A. Barbhuiya, and S. Nandi, "Online Voting System Powered By Biometric Security Using Steganography," in *Second International Conference on Emerging Applications of Information Technology*, India, 2011, pp. 112-139.
- [28] J. B. Nun, N. Farhi, M. Llewellyn, B. Riva, A. Rosen, A. Ta-Shma and D. Wikström, "A New Implementation of a Dual (Paper and Cryptographic) Voting System", India, 2003, pp. 110-125.
- [29] B. Adida, O. Demarneffe, O. Pereira and J. J. Quisquater, "Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios," in *Proceedings of the Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*, Montreal, Canada, 2009, pp. 122-134.
- [30] R. Araujo, R. F. Custodio and J. Van De Graaf, "A verifiable voting protocol based on farnel," *In Proceedings of the IAVoSS Workshop on Trustworthy Elections*, 2006, pp. 39-57.
- [31] J. Benaloh, "Simple verifiable elections," in *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop on Electronic Voting Technology Workshop*, USA: CA, 2006, pp. 122- 145.
- [32] M. Yung and J. Benaloh, "Distributing the power of a government to enhance the privacy of voters.," in *Proceedings of the Fifth ACM Symposium on Principles of Distributed Computing (PODC'86)*, New York, 1986, pp. 14-37.
- [33] D. Chaum, "Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting," *Security and Privacy, IEEE*, 2008, pp. 40-46.

- [34] R. Poovendran and K. Sampigethaya, "A framework and taxonomy for comparison of electronic voting schemes," in *computers & security* 25, USA, 2006.
- [35] P. Lei, S. Mao-hua, L. Shou-shan, W. Bai and X. Yang, "Full privacy preserving electronic voting scheme," *The Journal of China Universities of Posts and Telecommunications*, 2012, pp. 86–93.
- [36] A. Fujioka, T. Okamoto and K. Ohta, "practical secret voting scheme for large scale elections. Workshop on the Theory and Application of Cryptographic Techniques:," *Advances in Cryptology, Vol. 5*, 1992, pp. 57-76.
- [37] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections.," in *Proceedings of the Fifth International Workshop on Security Protocols*, 1997.
- [38] V. George and M. P. Sebastian, "An Efficient Homomorphic Coercion Resistant and E2E Verifiable Voting Scheme," *Computer and Information Science*, 2010, pp. 125-130.
- [39] E. Magkos, M. Burmester and V. Chrissikopoulos, "Receipt-freeness in large-scale elections without untappable channel," in *The first IFIP Conference on E-commerce/E-business/E-government*, Zurich, 2001.
- [40] J. Dossogne and F. Lafitte, "Blinded additively homomorphic encryption schemes for self-tallying voting," *Journal of Information Security and Applications* 22, 2015, pp. 40-53.
- [41] D. Chaum, "Blind Signatures for Untraceable Payments," *Crypto-82*, *n.d.*
- [42] C. David, "Untraceable Electronic Mail Return Addresses and Digital Pseudonyms," *Communications of the ACM* (24), 1981, pp. 84-88.
- [43] H. Jonker, S. Mauwa and J. Panga, "Privacy and verifiability in voting systems: Methods, developments and trends," *Computer Science Review* 10, 2013, pp. 1-30.
- [44] P. F. Syverson, D. M. Goldschlag and G. M. Reed, "Anonymous connections and onion routing, in: Proc. 18th IEEE Symposium on Security and Privacy, S&P," *IEEE Computer Society*, 1997, pp. 44–54.
- [45] P. Wolf, R. Nackerdien and D. Tuccinardi, "Introducing Electronic Voting: Essential Considerations," Chicago, 2011.
- [46] N. B. Silva, D. F. Pigatto, M. S. Paulo and K. R. Branco, "Case Studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer," *Journal of Network and Computer Applications*, 2015.
- [47] S. Kimbi and I. Zlotnikova,, " Citizens' Readiness for Remote Electronic Voting in Tanzania.," *Advances in Computer Science: an International Journal*, vol. 3, 2014, pp. 150-159.
- [48] M. Achieng and E. Ruhode,, "The Adoption and Challenges of Electronic Voting Technologies within The South African Context.," *International Journal of Managing Information Technology*, vol. 5, 2013, pp. 1-12.
- [49] M. Hapsara, "E-Voting Indonesia: A safety-critical-systems model towards standard and framework for Indonesia's presidential election.," in *In: International Conference on Information Technology*, Bali, Indonesia, 2013.
- [50] "Agency for Public Management and eGovernment (DIFI): MinID," April 2015. [Online]. Available:

<http://eid.difi.no/en/minid>. [Accessed 23 January 2018].

- [51] J. Rhodes, "The Chronicle of Evidence - Based Mentoring," 13 October 2014. [Online]. Available: <http://chronicle.umbmentoring.org/on-methods-whats-the-difference-between-qualitative-and-quantitative-approaches/>. [Accessed 07 May 2015].
- [52] R. L. Rivest, "Perspectives on end-to-end voting systems," Washington , 2009.
- [53] "Information Security Stack Exchange," 2013. [Online]. Available: <http://security.stackexchange.com/questions/9260/sha-rsa-and-the-relation-between-them>. [Accessed 27 April 2015].
- [54] K. Fisher and R. Carback, "Punchscan: Introduction and System Definition of a High-Integrity Election System," in *In Preproceedings of the IAVoSS Workshop on Trustworthy Elections (Robinson College, Cambridge, United Kingdom)*, United Kingdom, 2006.
- [55] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and digital Pseudonyms," *Communications of the ACM* (24), 1981, pp. 84-88.
- [56] M. Bellare and P. Rogaway, "The Exact Security of Digital Signatures - How to Sign with RSA and Rabin," in *Advances in Cryptology* , Spain, Springer Berlin Heidelberg, 1996, pp. 399-416.
- [57] T. Elgamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory* 31, 1985, pp. 469-472.
- [58] D. Chaum, . J. van de Graaf, P. Y. Ryan and P. L. Vora, "Secret Ballot Elections with Unconditional Integrity," in *Proceedings of the 8th ACM Conference on Computer and Communications Security, USA*, New York, 2007, pp. 95-135.
- [59] S. Krishna and R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes," *Computers & Security* 2 5, 2006, pp. 1 3 7 – 1 5 3.
- [60] A. Ben, "Helios Trust the Vote," 30 April 2016. [Online]. Available: <https://vote.heliosvoting.org/> [Accessed: 05/08/2016].
- [61] C. R. Kothari, "Research Methodology: Methods and Techniques," New Age Publication, New Delhi, 2004.
- [62] B. Adiba, 30 April 2016. [Online]. "Cryptography is a lot more than Blockchain" Available: <http://ben.adida.net/> [Accessed: 10/03/2017]
- [63] S. N. Burns and S. K. Grove, *The practice of nursing research*, Philadelphia: Saunders, 1997.
- [64] A. Miyaji, H. Kikuchi and K. Rannenberg, "In Advances in Information and Computer Security," in *Verifiable Internet Voting Solving Secure Platform Problem*, Heidelberg, 2007, pp. 199-213.
- [65] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *In Proceedings of CRYPTO 84 on Advances in cryptology*, New York, 1985.
- [66] A. J. Devegili, "Farnel: Uma proposta de protocolo criptografico para vota ´cao digital," Spain, 2001.
- [67] R. L. Rivest and W. D. Smith, "Three voting protocols: threeballot, VAV and twin," in *In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop*, 2007.

- [68] R. Rivest and W. D. Smith, "Three voting protocols: threeballot, VAV, and Twin," in *In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop*, 2007.
- [69] R. L. Rivest, "The ThreeBallot Voting System," 2006.
- [70] A. Borodzhieva and P. Manoilov , "Software Tool for Implementing RSA Algorithm," in *International Scientific Conference Computer Science*, Rousse, 2008, pp. 156- 197.
- [71] J. Nechvatal, "Public-Key Cryptography," Maryland, 1991.
- [72] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity," In *EUROCRYPT* (1999).
- [73] A. S. Schneider, A. P. Y. Ryan and D. Chaum, "A practical, voter-verifiable, election scheme, Report," University of Newcastle Upon Tyne, School of Computer Science, Newcastle, 2005.
- [74] G. Mateescu and M. Vladescu, "A Hybrid Approach of System Security for Small and Medium Enterprises: Combining different Cryptography techniques," in *Proceeding of the 2013 Federated Conference on Computer Science and Information Systems*, 2013, pp. 106-157.
- [75] O. M. Olaniyi, O. T. Arulogun and E. O. Omidiora, "Towards an Improved Stegano-Cryptographic Model for Secured Electronic Voting," *African Journal of Computing & ICT*, vol. 5, no. 6, 2012, pp. 10-16.
- [76] M. B. Abdullahi and O. Osho, "Framework for an E-Voting System Applicable in Developing Economies," *International Journal of Information Engineering and Electronics Business*, vol. 6, 2016, pp. 9-21.
- [77] B. C. Molokwu and M. N. Agu, "Secure Intranet Voting System for Students Union Elections in Nigeria Tertiary Institutions," *IOSR Journal of Computer Engineering*, vol. 16, no. 6, 2014, pp. 78-89.
- [78] S. Kimbi and I. Zlotnikova, "A Secure Model for Remote Electronic Voting: Case of Tanzania," *Advances in Computer Science: An International Journal*, vol. 3, no. 4, 2014, pp. 2322-5157.
- [79] M. O. Yinyeh, and K. Gbolagade, "Overview of Biometric Electronic Voting System in Ghana.," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, 2013, pp. 624-628.
- [80] W. M. Santos, R. J. de Queiroz, C. E. Saraiva and G. P. Junior, "Toward coercion-resistant end-to-end verifiable electronic voting systems," *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Brazil, 2013.
- [81] A. Bryman, "Integrating quantitative and qualitative research: How is it done?," *Qualitative Research*, no. 6, 2006, pp. 97–113.
- [82] J. W. Creswell, "Research design: Qualitative, quantitative, and mixed methods approaches," *Thousand Oaks, CA: Sage Publications*, 2013.
- [83] A. H. Onwuegbuzie and N. L. Leech, "Linking research questions to mixed methods data analysis procedures," *The Qualitative Report*, vol. I, no. 11, 2006, pp. 474–498.
- [84] R. B. Johnson, A. J. Onwuegbuzie and L. A. Turner, "Toward a definition of mixed methods research," *Journal of Mixed Methods Research*, vol. 1, 2007, pp. 112–133.

- [85] Authority, Fraser Health, "Quantitative Research Methods and Tools ©," 2011.
- [86] S. Elo and H. Kyngas, "The qualitative content analysis process," no. Cole 1988, USA, 2007, pp. 107-116.
- [87] R. Franzosi, "Content Analysis: Objective, Systematic, and Quantitative Description of Content," San Francisco 1956.
- [88] J. H. McMillan and S. Schumacher, *Research in Education: A Conceptual introduction*, New York: Harper Collions, 1993.
- [89] S. Merriam, *Qualitative research and case study applications in education*, San Francisco, 1998.
- [90] D. Jefferson, A. D. Rubin, B. Simons and D. Wagner, "A Security Analysis of the Secure Electronic," 20 January 2004. [Online]. Available: <http://servesecurityreport.org/> [Accessed: 12/09/2016].
- [91] S. Saini and J. Dhar, "An Eavesdropping Proof Secure Online Voting Model," *International Conference on Computer Science and Software Engineering*, 2008, pp. 704-708.
- [92] M. Q. Patton and M. Cochran, "Guide to using Qualitative Research Methodology," in *Research Unit, London School of Hygiene and Tropical Medicine*, United Kingdom, 2007.
- [93] K. Sampigethaya and R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes," in *computers & security* 25, USA, 2006.
- [94] K. Sampigethaya and R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes," *computers & security* 25, 2006, pp. 137 – 153.
- [95] Y. J. Lai, "Design and Implementation of an Electronic Voting System with Contactless IC Cards," 2008. [Online]. Available: http://59.127.136.65/publications/200805ICIM_eVoting.pdf. [Accessed 21 February 2016].
- [96] G. A. Kristian, "E-Voting and Identity: Third International Conference," in *The Norwegian Internet Voting Protocol*, Tallinn, Estonia, Springer Berlin Heidelberg, 2011, pp. 1-18.
- [97] C. Williams, "Research Methods," vol. 5, no. 3, 2007, pp. 65-72.
- [98] C. A. Neff, "Practical high certainty intent verification for encrypted votes, Report", Chicago, 2004.
- [99] S. Popoveniuc and B. Hosp, "An Introduction to Punchscan," in *An Introduction to Punchscan. In Preproceedings of the IAVoSS Workshop on Trustworthy Elections (Robinson College, Cambridge, United Kingdom, United Kingdom*, 2006.
- [100] A. C. Myers, M. Clarkson and S. Chong, "Civitas: Toward a secure voting System," *In IEEE Symposium on Security and Privacy*, 2008, pp. 354–368.
- [101] D. R. Sandler, K. Derr and D. S. Wallach, "VoteBox: a tamper-evident, verifiable electronic voting system," *In Proceedings of the 17th USENIX Security Symposium*, 2008.
- [102] K. Sal, "Remote Internet Voting and Increase of voter turnout: Happy coincidence or fact? The case of Estonia, Report," Czech Republic, 2015.
- [103] A. S. De Vos, H. Strydom, C. B. Fosche and C. S. L. Deport, "Research at grass roots: for the social sciences and human service professions" *Book, New York City(USA)*, vol. III, 2002.

- [104] A. Juels, M. Luby and R. Ostrovsky, "Security of Blind Digital Signatures, Journal," IEEE Security and Privacy, Brasov, Romania, vol. II, 2014, pp. 99-120.
- [105] T. Adeyinka and G. Olasina, Voter's Perception of the Adequacy and Suitability of e-Voting in the Nigeria Polity. In: Handbook of Research on E-Government in Emerging Economies: Adoption, e-participation, and legal frameworks, IGI Global, 2012.
- [106] C. Kuye, J. Coker, I. Ogundeinde and C. Coker, "Design and Analysis of Electronic Voting System in Nigeria," *International Archive of Applied Sciences and Technology*, no. 4, 2013, pp. 15-20.
- [107] S. Ishaq, W. Osman, A. Shittu and . R. Jimoh, "Adoption of E-Voting System in Nigeria: A conceptual framework.," *International Journal of Applied Information Systems*, vol. 5, 2013, pp. 8-14.
- [108] M. Musa and F. Aliyu, "Design of Electronic Voting Systems for Reducing Election Process.," *International Journal of Recent Technology and Engineering*, vol. 2, 2013, pp. 183-186.
- [109] O. Olaniyi, O. Arulogun and E. Omidiora, "Design of Secure Electronic Voting System using Multifactor Authentication and Cryptographic Hash Function.," *International Journal of Computer and Information Technology*, vol. 2, 2013, pp. 1122-1130.
- [110] S. Adeshina, "Towards Improved Adoption of e-Voting - Analysis of the case of Nigeria.," in *8th International Conference on Theory and Practice of Electronic Governance*, Portugal, 2014, pp. 7-23.
- [111] S. Folarin, C. Ayo, A. Oni and D. Gberevbie, "Challenges and Prospects of e-Elections in Nigeria.," in *European Conference on eGovernment*, Brasov: Romania, 2014, pp. 23-35.
- [112] N. Iromini, H. Onawola and A. Ajao, "Electronic Voting System for Student Election Process.," *International Journal of Computer & Communication Engineering Research*, vol. 2, 2014, pp. 183-192.
- [113] O. Olaniyi, O. Arulogun, E. Omidiora and O. Okediran, "Performance Assessment of an Imperceptible and Robust Secured E-Voting Model.," *International Journal of Scientific & Technology Research*, vol. 3, 2014, pp. 127-132.
- [114] M. Hapsara, "Electronic Voting for the People of Mount Merapi, Really?," in *IEEE International Symposium on Technology Management and Emerging Technology*, Bandung, Indonesia, 2014, pp. 10-16.
- [115] G. Abandah, K. Darabkh , T. Ammari and O. Qunsul, "Secure National Electronic Voting System.," *Journal of Information Science and Engineering*, vol. 30, 2013, pp. 1339-1364.
- [116] S. Kimbi, Y. Nkansah-Gyekye and K. Michael, "Towards a Secure Remote Electronic Voting in Tanzania - Organizational challenges," *Advances in Computer Science: an International Journal*, vol. 3, 2014, pp. 122-131.
- [117] I. R. Salimonu, S. O. B. Wan Rozaini, K. S. Abdul Jaleel and G. R. Jimoh, "Adoption of E-Voting System in Nigeria: A Conceptual Framework," *International Journal of Applied Information Systems (IJAIS)*, vol. 5, no. 5, 2013, pp. 8-14.

APPENDICES

Appendix A –Questionnaire Sample for Security and Election Experts

Demographic Information

“Please answer by ticking the most appropriate option”

Q1. Please select your age range

- ☐ 25 and below ☐ 26 – 35 ☐ 36 – 45 ☐ 46 and above

Q2. What is your gender?

- ☐ Male ☐ Female

Q3. What is your highest level of education?

- ☐ High school or less ☐ Some college ☐ Bachelor’s degree ☐ Master’s degree ☐ PhD

Q4. What is your position?

- ☐ Administration officer ☐ IT Officer ☐ Systems Analyst ☐ Top level management

If other (specify), _____

Q5. How long have you been with this organization?

- ☐ 1 - 5 years ☐ 6 – 10 years ☐ Above 10 years

Research related Questions

Q6. How will rate your level of understanding of e-voting system?

- ☐ Very high ☐ High ☐ Medium ☐ Low ☐ No knowledge

Q7. In your own professional opinion, do you think the current paper-based voting system has problems?

- ☐ Yes ☐ No ☐ Not sure

Explain,

Q8. Can E-voting reduce election problems encountered in Botswana?

☐ Yes ☐ No ☐ Not sure

Q9. Are you willing to use e-voting system if introduced?

☐ Yes ☐ No

Q10. Can you rely on the results of an e-voting system?

☐ Yes ☐ No

Objective One: “Potential Benefits of introducing E-voting in Botswana”

In your opinion what are the potential benefits of e-voting introduction and implementation?

(On a scale of 1 to 5; 1- Strongly Agree, 2- Agree, 3- Not sure, 4-Disagree 5- Strongly Disagree)

Q11 – Q16	1	2	3	4	5
11.E-Voting will speed up the process of voting since the process to go through before voting will be reduced					
12. E-voting will increase the number of respondents if introduce, hence increasing voter turnout.					
13. E-Voting will reduce delays in vote counting					
14. E-Voting will eliminate voting fraud (eg. Multiple voting, vote rigging etc.)					
15. E-voting will reduce the chances of spoilt votes					
16. E-voting will eliminate error during vote counting due to manual counting and fatigue					

If any, specify,

Objective Two: “Potential Security Challenges that hinders implementation of e-voting in Botswana”

Do you believe the following challenges can affect the implementation of E-Voting?
(On a scale of 1 to 5; 1- Strongly Agree, 2- Agree, 3- Not sure, 4-Disagree 5- Strongly Disagree)

Q17 – Q26	1	2	3	4	5
17. IEC staff do not have enough skill set to support and manage implementations of e-voting					
18. They are lack of ICT resources by IEC to support E-Voting system					
19. Unstable communication link during election period					
20. E-voting system can fail on election days due to system failure or software bugs					
21. Power outages at polling station during voting period will disrupt elections					
22. Security Issues (Insider hacking into the system, voter anonymity etc.)					
GENERAL FACTORS					
23. Cost of implementing e-voting will be high					
24. E-voting will be difficult to be used due to high illiteracy rate					
25. Difficulty of voters to confirm that what they voted is what is recorded by the system					
26. Voters will find user interface cumbersome to use					

Other security challenges, (specify), _____

“Thanks for your time and help”

Appendix B–Questionnaire Sample for Voting population

Demographic

“Please answer by ticking the most appropriate option”

Q1. Please select your age range

- ☐ 25 and below ☐ 26 – 35 ☐ 36 – 45 ☐ 46 and above

Q2. What is your gender?

- ☐ Male ☐ Female

Q3. What is your highest level of education?

- ☐ High school or less ☐ Some college ☐ Bachelor’s degree ☐ Master’s degree ☐ PhD

Objective One: “Assessing the current situation and the problem”

Q4. Have you ever voted in any general elections in Botswana?

- ☐ Yes ☐ No

Q5. Have you ever heard about E-Voting?

- ☐ Yes ☐ No

Q6. In your own opinion do you think the current paper-based system has problems?

- ☐ Yes ☐ No ☐ Not Sure

Q7. Do you think the introduction of e-voting will solve election problems in Botswana?

- ☐ Yes ☐ No ☐ Not Sure

Q8. Do you think it is necessary to introduce e-voting in Botswana?

- ☐ Yes ☐ No

Q9. Are you willing to use e-voting if introduced?

- ☐ Yes ☐ No

Q10. Can you rely on the results of an e-voting system?

- ☐ Yes ☐ No

Q11. What voting technology will you prefer?

☐ Paper-Based Voting

☐ E-Voting

Q12. How will you rate your computer experience?

☐ Expert

☐ Advance

☐ Average

☐ Basic

☐ No
experience

Objective One: “Potential Benefits of introducing e-voting in Botswana”

In your opinion what are the potential benefits of e-voting introduction and implementation?

(On a scale of 1 to 5; 1- Strongly Agree, 2- Agree, 3- Not sure, 4-Disagree 5-Strongly Disagree)

Q13 – Q18	1	2	3	4	5
E-Voting will speed up the process of voting since the process to go through before voting will be reduced					
E-voting will increase the number of respondents if introduce, hence increasing voter turnout.					
E-Voting will reduce delays in vote counting					
E-Voting will eliminate voting fraud (eg. Multiple voting, vote rigging etc.)					
E-voting will reduce the chances of spoilt votes					
E-voting will eliminate error during vote counting due to manual counting and fatigue					

“Thanks for your time and help”