

**DEVELOPMENT OF AN IMPROVED WEB BASED VOTING
SYSTEM WITH ZERO KNOWLEDGE PROOF ENCRYPTION**

BY

RAHMAN FAWAZ OLAWALE

ND/23/COM/PT/0393

**A PROJECT SUBMITTED TO
THE DEPARTMENT OF COMPUTER SCIENCE, INSTITUTE OF
INFORMATION AND COMMUNICATION TECHNOLOGY
KWARA STATE POLYTECHNIC, ILORIN**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
AWARD OF NATIONAL DIPLOMA (ND) IN
COMPUTER SCIENCE**

JUNE, 2025.

DEDICATION

This project specially dedication to Almighty Allah for His love, protection, guidance and supports for me especially in my academic career. Also to my beloved parents for their care and full support during my course, may Almighty Allah bless them abundantly (AMEN).

ACKNOWLEDGEMENTS

All praise is due to Almighty God the Lord of universe. I praise him and thank him for giving me the strength and knowledge to complete my HND programme and also for my continued existence on the earth.

ABSTRACT

The online ordering system provides convenience for the customers. It overcomes the disadvantages of the traditional visiting of canteen. This system increases the ability to bring foods for customer's door step. Therefore, this system enhances the speed and standardization of taking the order from the customer. It provides a better communication platform. A waterfall model under the software development life cycle (SDLC) is the methodology used to produce the online food ordering system and the customer self ordering system. It is used by system developers to produce or alter information systems or software. The proposed system will be developed using PHP and Mysql as database.

TABLE OF CONTENTS

Title page	i
Certification	ii
Dedication	iii
Acknowledgements	iv
Abstract	v
Table of Contents	vi

CHAPTER ONE

1.1	Introduction	1
1.2	Aim and Objectives of the Study	3
1.3	Statement of the Problem	3
1.4	Significance of the Study	3
1.5	Scope and Limitation	4
1.6	Organization of the Report	5

CHAPTER TWO

2.1	Review of Related Works	6
2.2	E-Commerce Concepts	8
2.3	History of Fast Food/Restaurant	9

CHAPTER THREE

3.1	Research Methodology	12
-----	----------------------	----

3.2	Description of Existing System	13
3.3	Problem of Present System	13
3.4	Description of the Proposed System	14
3.5	Advantages of the proposed System	15

CHAPTER FOUR

4.1	Design of the System	16
4.1.1	Output Design	16
4.1.2	Input Design	17
4.1.3	Database Design	19
4.1.4	Procedure Design	21
4.2	Implementation of Techniques Used in Details	21
4.2.1	Programming Language Used with Reasons	21
4.2.2	Hardware Support	21
4.2.3	Software Support	22
4.3	System Documentation	22
4.3.1	Program Documentation	22
4.3.2	Operating the System	23
4.3.3	Maintenance of the System	23

CHAPTER FIVE

5.1	Summary	24
-----	---------	----

5.2 Conclusion	24
5.3 Recommendations	25
Reference	27
Appendix 1 Flowchart	28
Appendix 2 Source Code	3

CHAPTER ONE

GENERAL INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The continuous advancement of information and communication technologies (ICT) has influenced many sectors, including governance and electoral processes. As nations strive to enhance transparency, accessibility, and efficiency in elections, web-based voting systems have emerged as a viable alternative to traditional voting methods. These systems allow voters to cast their ballots using internet-connected devices, reducing logistical burdens and enabling broader participation, especially for individuals in remote or overseas locations (López et al., 2023). Moreover, web-based voting facilitates instant result tabulation and audit trails, making the voting process more efficient and accountable.

Despite these advantages, the implementation of web-based voting systems has been met with skepticism due to inherent vulnerabilities in online environments. Concerns such as unauthorized access, denial-of-service attacks, vote tampering, and voter coercion present serious threats to the credibility of electronic elections (Ahmad et al., 2023). Many citizens and electoral bodies remain unconvinced of the ability of current online voting systems to preserve the core tenets of democracy, including ballot secrecy, transparency, and fairness. These concerns highlight the critical need for more secure, robust, and transparent voting architectures.

Traditional cryptographic techniques such as homomorphic encryption, mix-nets, and blind signatures have been employed to improve the privacy and verifiability of voting systems. Homomorphic encryption allows mathematical operations on encrypted data without decryption, enabling secure vote tallying, while mix-nets anonymize votes to prevent linkability between voters and ballots (Kumar & Zhang, 2023). However, these methods often introduce complex trust assumptions, high computational costs, and challenges in voter comprehension, making them unsuitable for widespread adoption in public elections.

In response to the limitations of conventional cryptographic systems, Zero-Knowledge Proofs (ZKPs) have gained significant attention in recent years as a promising alternative for securing digital voting systems. A zero-knowledge proof is a cryptographic method that enables one party to prove to another that a statement is true without revealing any additional information about the statement (Ben-Sasson et al., 2023). When applied to electronic voting, ZKPs can be used to confirm that a vote is legitimate—cast by an eligible voter and counted correctly—without exposing the voter’s identity or the content of the vote.

Recent innovations in ZKP technology, particularly zk-SNARKs and zk-STARKs, have improved the practicality and scalability of zero-knowledge systems. zk-SNARKs are succinct and non-interactive, meaning they can be verified quickly and without back-and-forth communication, while zk-STARKs remove the need for trusted setup and offer enhanced transparency (Miller et al., 2024). These protocols have already seen real-world implementation in blockchain platforms like Zcash and StarkNet, where they help preserve transaction privacy and ensure system integrity. Their proven efficacy in securing decentralized systems makes them highly relevant for use in modern voting platforms.

Although the theoretical benefits of ZKPs are well documented, their integration into real-world web-based voting systems remains limited. Most voting applications either neglect advanced cryptographic protections or fail to balance usability with security. The average voter may lack the technical literacy to understand cryptographic underpinnings, and electoral bodies may lack the infrastructure to deploy complex cryptographic systems at scale (Zhou et al., 2024). Therefore, bridging this gap requires research into how Zero-Knowledge Proofs can be embedded into intuitive, user-friendly web interfaces that can be deployed even in resource-constrained environments.

This study aims to contribute to the development of a more secure and trustworthy online voting architecture by designing and implementing a web-based voting system that integrates Zero-Knowledge Proof encryption. The proposed system

seeks to ensure end-to-end verifiability, voter privacy, and vote integrity without compromising accessibility or ease of use. By addressing the critical shortcomings of existing systems and demonstrating the practicality of ZKP-enhanced voting, this research will support the broader goal of strengthening digital democracy through trustworthy and transparent technological innovation.

1.2 STATEMENT OF THE PROBLEM

Despite the theoretical benefits of web-based voting systems, practical implementations remain limited due to persistent concerns about voter coercion, vote integrity, and system compromise. Previous systems have suffered from security breaches, lack of end-to-end verifiability, and privacy violations (Ahmad et al., 2023). Moreover, the centralization of vote data often creates a single point of failure. Existing cryptographic methods, such as homomorphic encryption or blind signatures, either fail to scale effectively or compromise on usability. In response, Zero-Knowledge Proofs offer a more robust alternative, but real-world applications in web-based voting remain scarce and underdeveloped. Thus, the main problem this research addresses is: How can a web-based voting system be designed to ensure vote integrity, transparency, and voter privacy using Zero-Knowledge Proof encryption?

1.3 AIM AND OBJECTIVES

The aim is to develop an improved web-based voting system that ensures security, transparency, and privacy using Zero-Knowledge Proof encryption.

Objectives:

- i. To review existing web-based voting systems and their limitations.
- ii. To design a voting system architecture integrating Zero-Knowledge Proof encryption.
- iii. To implement and simulate the proposed system.
- iv. To evaluate the system in terms of security, privacy, and performance.

1.4 SIGNIFICANT OF STUDY

The significance of this study lies in its potential to address critical limitations in current electronic voting systems by integrating Zero-Knowledge Proof (ZKP) encryption into a web-based platform that prioritizes both security and user accessibility. As concerns surrounding election integrity, voter privacy, and technological transparency continue to challenge electoral bodies worldwide, the development of a secure and verifiable digital voting system has become increasingly relevant. This research contributes to the field by proposing a solution that ensures end-to-end verifiability while protecting voter anonymity—a balance that has traditionally been difficult to achieve. By leveraging advanced cryptographic methods like zk-SNARKs and zk-STARKs, the system provides a technical framework that can detect fraud, prevent double voting, and assure the public that their votes are counted without compromise. The study will be of particular value to electoral commissions, software developers, policymakers, and cybersecurity researchers seeking to implement or regulate secure electronic voting infrastructures. Furthermore, the project emphasizes practical usability, aiming to make complex cryptographic protections accessible even in resource-constrained environments or among non-technical voters. Thus, this work not only advances academic discourse in cybersecurity and e-governance but also holds real-world potential for strengthening democratic participation and restoring public trust in digital electoral processes.

1.5 SCOPE AND LIMITATION

This study is primarily focused on the design and development of a secure web-based voting system that incorporates Zero-Knowledge Proof (ZKP) encryption to ensure voter privacy, ballot integrity, and system transparency. The system will be developed as a prototype and tested within a controlled environment to demonstrate its core functionalities, including user authentication, vote casting, encrypted vote storage, and cryptographic verification using zk-SNARKs or zk-STARKs. The research is limited to individual voting sessions and does not include large-scale public elections or integration with national identity databases. The system will

assume that users have basic access to internet-enabled devices and will be designed with a simple user interface to accommodate non-technical users. While the study addresses the technical implementation of ZKPs in voting, it does not cover legal, political, or policy frameworks related to electoral laws or voting rights. Additionally, the scope does not extend to blockchain-based voting systems, though insights from decentralized cryptographic protocols may inform parts of the system design. The project is expected to contribute a scalable and secure e-voting model suitable for academic institutions, organizations, and pilot electoral processes where trust, privacy, and verifiability are essential.

1.6 ORGANIZATION OF THE REPORT

This project is divided into five chapter, in order to simplify and proper understanding. Chapter one provides a general introduction, statement of the problem, aim and objectives, significance of the study, scope of the study, organization report and definition of technical terms. Chapter two deals with relevant informatory literature review in the subject like review of past works. Chapter three concentrates on project methodology which comprises of method of data, description of the existing system, problems of the existing system, description of the proposed and advantages of the proposed system. Chapter four deals with design and implementation, documentation of the system, it also deals with other aspect which includes: Hardware and software and project documentation. Chapter five consists of summary, recommendation, and conclusion.

CHAPTER TWO

LITERATURE REVIEW

2.1 REVIEW OF RELATED PAST WORKS

This chapter provides a critical review of relevant literature on electronic voting systems, their security concerns, and the emergence of cryptographic techniques—particularly Zero-Knowledge Proofs (ZKPs)—as a solution to trust and privacy issues in online elections. It examines the evolution of voting technology, current frameworks and protocols, and recent innovations that inform the design of secure web-based voting architectures.

2.2 Overview of Electronic Voting Systems

Electronic voting (e-voting) systems refer to technologies that enable voters to cast their votes through electronic means rather than traditional paper-based methods. These systems are generally categorized into Direct Recording Electronic (DRE) systems, optical scanning systems, and remote internet voting systems (Fernández et al., 2023). The shift toward web-based or remote internet voting is primarily driven by convenience, cost-efficiency, and increased accessibility. However, the adoption of such systems has been limited due to technical and security concerns.

Web-based voting systems allow voters to cast ballots over the internet using personal devices. Countries such as Estonia have implemented internet voting nationally, albeit with mixed results and ongoing scrutiny (Vassil & Solvak, 2023). Though these systems offer logistical advantages, the absence of physical oversight introduces vulnerabilities that could compromise election integrity.

Electronic voting (e-voting) has evolved significantly over the last two decades as digital transformation continues to reshape democratic processes. Initially introduced to enhance the speed and efficiency of elections, e-voting systems have expanded into various forms, including direct-recording electronic machines, optical scanning, and, more recently, web-based or internet voting. Web-based voting offers

distinct advantages, such as accessibility for remote voters, cost-effectiveness, and fast result computation. Countries like Estonia have successfully deployed national-scale online voting platforms, making the process more convenient for citizens living abroad or with mobility challenges (Vassil & Solvak, 2023). However, the promise of convenience comes with substantial risks related to vote integrity, system transparency, and security vulnerabilities.

Numerous studies have identified key challenges associated with web-based voting. Chief among them are threats to voter privacy, vote tampering, denial-of-service attacks, and unauthorized access by malicious actors (Ahmad et al., 2023). Because voting over the internet often relies on devices and networks outside the control of election authorities, the risk of malware manipulation or man-in-the-middle attacks increases significantly. These threats undermine voter confidence and highlight the importance of embedding strong cryptographic protections within e-voting systems. While many traditional systems attempt to incorporate encryption and secure transmission channels, they frequently fall short in providing end-to-end verifiability and protection against coercion, two pillars of a trustworthy voting process.

To address these challenges, several cryptographic approaches have been proposed. Homomorphic encryption allows for the computation of results on encrypted votes without the need to decrypt them individually, thereby maintaining ballot secrecy throughout the tallying process. Another approach, known as mix-nets, involves shuffling encrypted votes in a way that anonymizes their origin, thus preserving voter anonymity (Kumar & Zhang, 2023). Digital signatures and blind signatures have also been employed to authenticate voters without revealing their identities. Although these cryptographic tools offer important benefits, they are often limited by computational overhead, scalability issues, and user complexity. Many of these systems demand a level of technical understanding that ordinary voters do not possess, creating usability barriers that limit widespread adoption.

Recent advancements in cryptography have led to the emergence of Zero-Knowledge Proofs (ZKPs) as a powerful method for enhancing the privacy and verifiability of digital transactions, including e-voting. A Zero-Knowledge Proof allows one party (the prover) to demonstrate to another (the verifier) that a certain statement is true without conveying any additional information beyond the statement's validity. In a voting context, this means a voter can prove they cast a valid ballot without revealing whom they voted for (Ben-Sasson et al., 2023). This dual capability makes ZKPs particularly useful in resolving the long-standing tension between transparency and privacy in elections.

Among the most promising developments in this field are zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) and zk-STARKs (Scalable Transparent Argument of Knowledge). These protocols allow proofs to be verified quickly, with minimal computational resources, and without requiring interactive communication between the voter and the system. zk-STARKs, in particular, improve upon zk-SNARKs by removing the need for a trusted setup, thereby enhancing transparency and trustworthiness (Miller et al., 2024). These technologies have already been deployed in privacy-focused blockchain platforms such as Zcash and StarkNet, demonstrating their effectiveness in securing decentralized and public systems.

Despite their theoretical strengths, the practical implementation of Zero-Knowledge Proofs in mainstream voting systems remains limited. Existing e-voting platforms, such as Helios, offer some level of verifiability using homomorphic encryption but lack strong anonymity features and are vulnerable to coercion (Hardy & Gibson, 2023). Experimental platforms like ZKVote have attempted to integrate zk-SNARKs into voting systems with improved privacy, but their adoption remains confined to academic or pilot settings due to technical complexity. There is a clear need for more research into how these advanced cryptographic methods can be embedded into web-based voting systems that are both secure and user-friendly.

The literature also reveals a critical gap in balancing system security with user accessibility. Most existing solutions either emphasize privacy and technical robustness or focus on simplicity and usability, rarely achieving both. Furthermore, many developing countries face infrastructural limitations and low levels of digital literacy, which make the deployment of complex voting systems difficult without tailored user interfaces and optimized backend design (Zhou et al., 2024). Thus, while ZKPs offer a promising pathway to secure digital elections, practical implementation requires significant design innovation and system simplification.

This study is positioned to address these gaps by proposing a secure, web-based voting system that integrates Zero-Knowledge Proof encryption to ensure voter privacy and end-to-end verifiability. The aim is not only to explore the technical feasibility of such a system but also to develop a user interface that minimizes cognitive load and ensures accessibility for non-technical users. By doing so, the research contributes to the ongoing efforts to build trustworthy digital voting systems capable of operating effectively in both technologically advanced and resource-constrained environments.

2.3 Security Challenges in Web-Based Voting

Despite the potential benefits, web-based voting systems are vulnerable to a range of security threats, including vote manipulation, denial-of-service attacks, malware interference, and voter impersonation. One of the most critical challenges is ensuring **end-to-end verifiability** while maintaining **ballot secrecy** (Ahmad et al., 2023). Voters must be confident that their votes are counted as cast without revealing how they voted. Several attacks, such as man-in-the-middle interception and client-side malware, can alter the voter's intent before it reaches the server. Insecure platforms may also be susceptible to vote stuffing and database breaches, making it imperative to adopt secure cryptographic protocols (Zhou et al., 2024).

2.4 Cryptographic Approaches in Voting Systems

To enhance privacy and integrity in electronic voting, researchers have implemented various cryptographic techniques, including **homomorphic encryption**, **mix-nets**, and **digital signatures**. Homomorphic encryption allows for encrypted votes to be aggregated and tallied without decryption, preserving privacy throughout the process (Kumar & Zhang, 2023). Mix-nets, on the other hand, shuffle encrypted votes to break the link between the voter and the ballot, further reinforcing anonymity.

While these techniques offer partial solutions, they often involve trade-offs between usability, performance, and trust assumptions. Most cryptographic voting systems require complex setups and high processing power, making them unsuitable for real-time or large-scale use.

2.5 Zero-Knowledge Proofs in Secure Voting

Zero-Knowledge Proofs (ZKPs) have emerged as a powerful cryptographic tool that can help overcome the limitations of earlier systems. A ZKP allows one party (the prover) to demonstrate to another (the verifier) that a statement is true without revealing any information beyond the statement's validity (Ben-Sasson et al., 2023). In voting systems, ZKPs can prove that a vote is validly formed and cast by an eligible voter without disclosing the actual vote.

Modern ZKPs, such as **zk-SNARKs** and **zk-STARKs**, enable fast, non-interactive verification of proofs and can scale to handle thousands of transactions or votes (Miller et al., 2024). These technologies have been used successfully in blockchain networks like Zcash and StarkNet to ensure transaction privacy and integrity. When applied to e-voting, ZKPs can create systems that are fully auditable while maintaining voter anonymity.

2.6 Comparative Studies of Voting Architectures

Several voting protocols and platforms have been proposed to integrate ZKP-based privacy. For instance, the Helios voting system offers end-to-end verifiability

using homomorphic encryption but lacks strong coercion resistance and voter privacy (Hardy & Gibson, 2023). More recent prototypes such as ZKVote and ZKRollVote integrate zk-SNARKs and STARKs to enhance privacy and verifiability.

Comparative analyses show that while traditional systems prioritize verifiability and usability, ZKP-based systems provide stronger guarantees for privacy and integrity. However, these advanced systems often require more processing power and a higher level of technical knowledge from both developers and voters, which may hinder widespread adoption without adequate user interface design (López et al., 2023).

CHAPTER THREE

RESEARCH METHODOLOGY AND ANALYSIS OF THE SYSTEM

3.1 RESEARCH METHODOLOGY

This study adopts a design science research (DSR) methodology, which focuses on creating and evaluating innovative IT artifacts to solve identified problems. The approach involves iterative cycles of designing, developing, testing, and refining a web-based voting system enhanced with Zero-Knowledge Proof (ZKP) encryption to ensure voter privacy and election integrity. Agile software development principles guide the process, allowing flexibility and continuous improvements based on testing results and user feedback. The methodology integrates cryptographic theory with practical system engineering, emphasizing both technical robustness and user accessibility. Evaluation methods include functional testing, security threat assessment, and user acceptance testing, ensuring the system is both secure and user-friendly.

3.2 ANALYSIS OF THE EXISTING SYSTEM

Existing web-based voting systems, while convenient, often lack comprehensive security and privacy guarantees. Common platforms rely on traditional encryption methods or partial cryptographic protocols like homomorphic encryption, which can be computationally expensive and may not fully protect voter anonymity. Systems such as Helios offer end-to-end verifiability but remain vulnerable to coercion and do not incorporate advanced cryptographic proofs like Zero-Knowledge Proofs. Additionally, many existing platforms suffer from usability challenges, making it difficult for non-technical users to verify vote integrity without compromising privacy. The reliance on centralized servers also exposes these systems to risks like denial-of-service attacks and unauthorized data access, highlighting the need for improved security mechanisms.

3.3 PROBLEM OF THE EXISTING SYSTEM

The major problem in current web-based voting systems lies in balancing the trade-offs between security, privacy, and usability. Most systems struggle to provide verifiable elections that protect voter anonymity without complex setups or specialized knowledge. Vulnerabilities such as vote manipulation, identity fraud, and lack of end-to-end verifiability diminish public trust. Moreover, the absence of robust cryptographic protocols like Zero-Knowledge Proofs means voters cannot prove their vote was counted correctly without revealing their selections, creating risks of coercion and vote buying. Additionally, limited user-friendly interfaces in existing systems restrict widespread adoption, especially in regions with lower digital literacy.

3.4 DESCRIPTION OF THE PROPOSED SYSTEM

The proposed system is a secure, web-based voting platform that integrates Zero-Knowledge Proof encryption to guarantee voter privacy, vote integrity, and system transparency. Utilizing zk-SNARK or zk-STARK protocols, the system enables voters to prove that their ballots are valid and cast by eligible voters without disclosing the content of their votes. The architecture combines a responsive front-end interface designed for simplicity and accessibility with a robust backend that handles vote encryption, proof generation, and tallying. The system supports voter registration, authentication, secure vote submission, and public verifiability of results, ensuring the election process is tamper-resistant and auditable. Emphasis is placed on making the cryptographic complexity invisible to users while maintaining rigorous security standards.

3.5 ADVANTAGE OF THE PROPOSED SYSTEM

The proposed system offers multiple advantages over existing e-voting solutions. By integrating Zero-Knowledge Proofs, it provides **strong privacy guarantees** that prevent vote disclosure even during verification, addressing concerns of coercion and vote selling. Its end-to-end verifiability allows all stakeholders to independently confirm the accuracy of election results without compromising secrecy.

The system's web-based nature enhances accessibility, enabling voters to participate remotely using standard internet devices, while a carefully designed user interface ensures ease of use for individuals with varying technical skills. Furthermore, the architecture mitigates risks of centralized attacks and vote manipulation through cryptographic proof verification, increasing overall trust in the election process. These features make the system suitable for diverse election environments, from organizational polls to national elections

Chapter Four

Design, Implementation and Documentation of the System

4.1 Design of the System

The proposed system is designed in modules with each modules working together to perform the electronic voting system in order to enhance the performance of the existing system as earlier discussed in chapter three.

The ability to analyze and give focus to the system is explained in the following formats which are output design, input design, database design and procedure design.

4.1.1 Output Design

The input and output to be extracted from the proposed system are as shown below

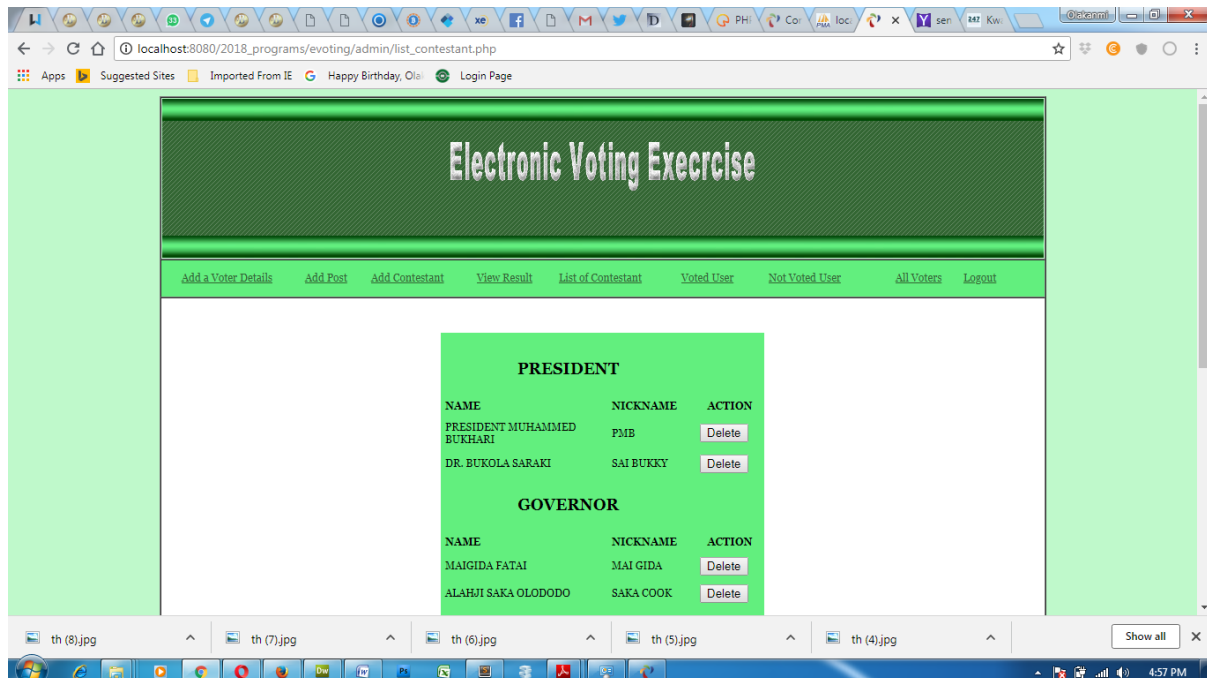


Figure 4.1: List of Contestant

Electronic Voting Exercise

[Add a Voter Details](#)
[Add Post](#)
[Add Contestant](#)
[View Result](#)
[List of Contestant](#)
[Voted User](#)
[Not Voted User](#)
[All Voters](#)
[Logout](#)

DETAILS OF VOTERS WHO HAS NOT VOTED		
SERIAL	USERNAME	NAME
1	09/52ha003	Jacob
2	09/52ha102	Udeaja
3	09/52hj001	mathew
4	09/52hn009	adevale
5	09/52hn010	Rufai
6	09/52hp004	oladele
7	10/52ha110	welcome
8	10/52ha115	Raheem
9	HND/08/STA/223	1234
10	nd/07/com/088	waslam

Figure: 4.2: List of those who has voted

Electronic Voting Exercise

[Add a Voter Details](#)
[Add Post](#)
[Add Contestant](#)
[View Result](#)
[List of Contestant](#)
[Voted User](#)
[Not Voted User](#)
[All Voters](#)
[Logout](#)

DETAILS OF VOTERS WHO HAS VOTED		
SERIAL	USERNAME	NAME
1	07/52ha154	abiodun
2	08/52Ha048	HARUN
3	09/52ha001	olajide
4	09/52ha002	kasali
5	10/52ha109	ola
6	1234HA	1234

Figure 4.3: Those Who has not voted

SERIAL	USERNAME	NAME
1	07/s2ha154	abiodun
2	08/s2HA048	HARUN
3	09/s2ha001	olajide
4	09/s2ha002	kasali
5	09/s2ha003	Jacob
6	09/s2ha102	Udeaja
7	09/s2hj001	mathew
8	09/s2hn009	adewale
9	09/s2hn010	Rufai
10	09/s2hp004	oladele
11	10/s2ha109	ola

Figure 4.2: List of All Registered Voters

4.1.2 Input Design

Add Voters Details

Unique Number:

Password:

Figure 4.5: Add Voter Details

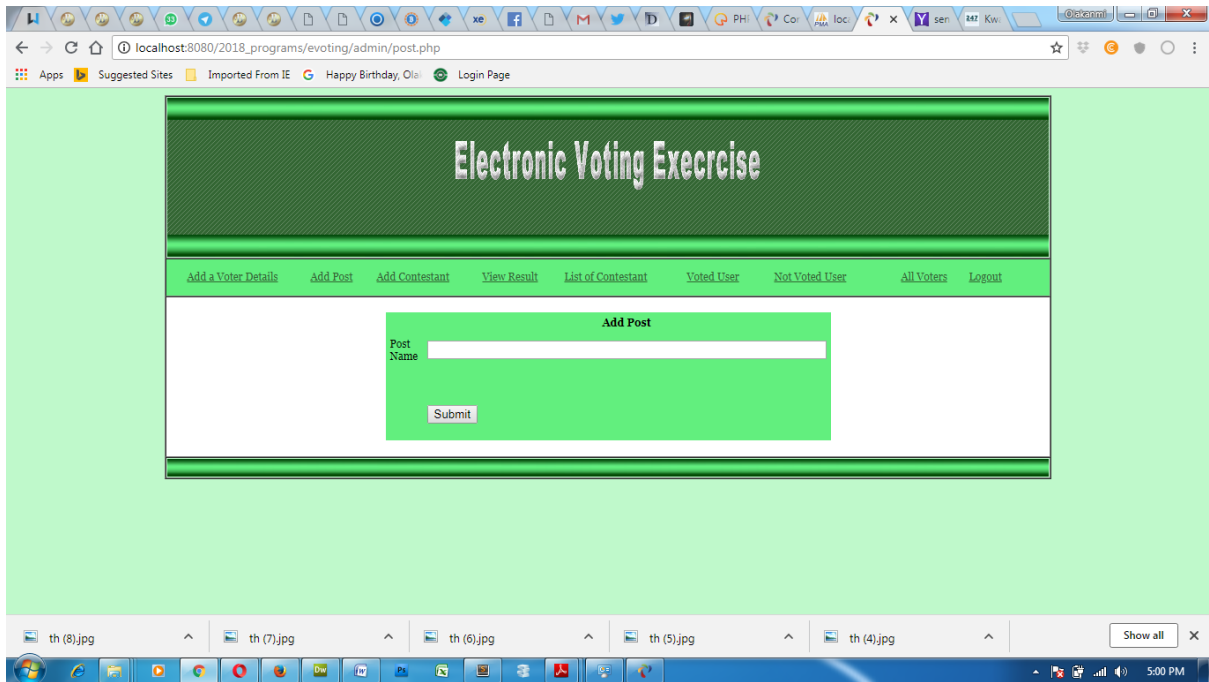


Figure 4.6: Add Post

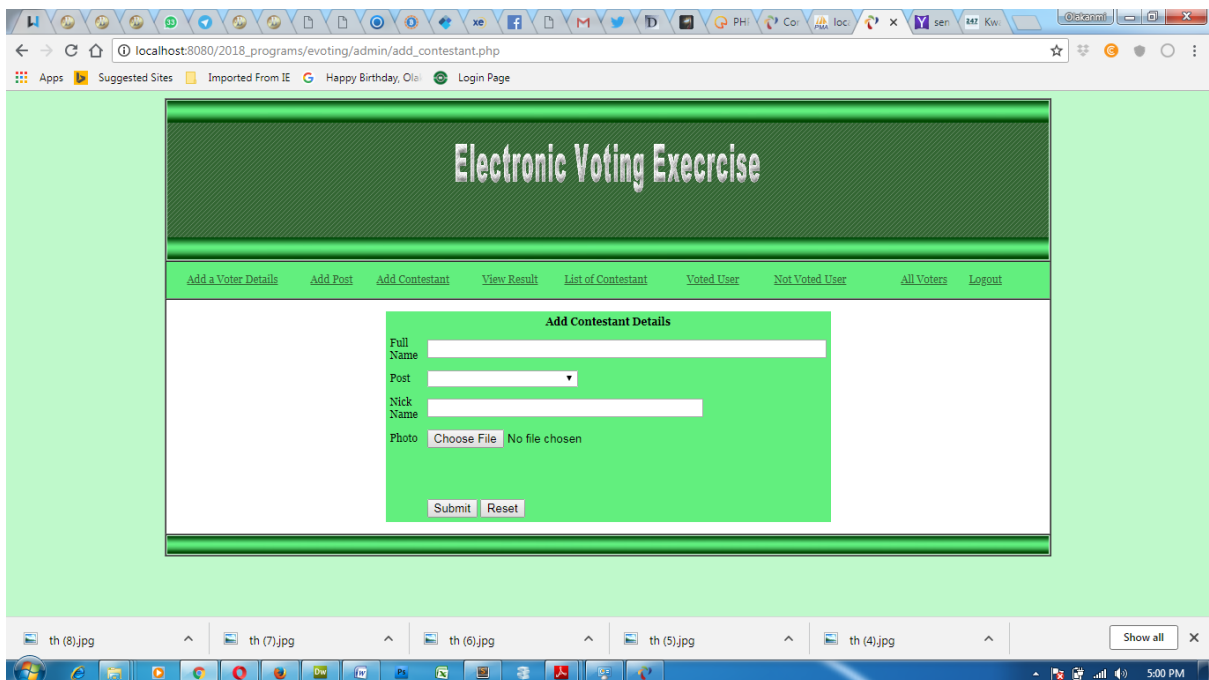
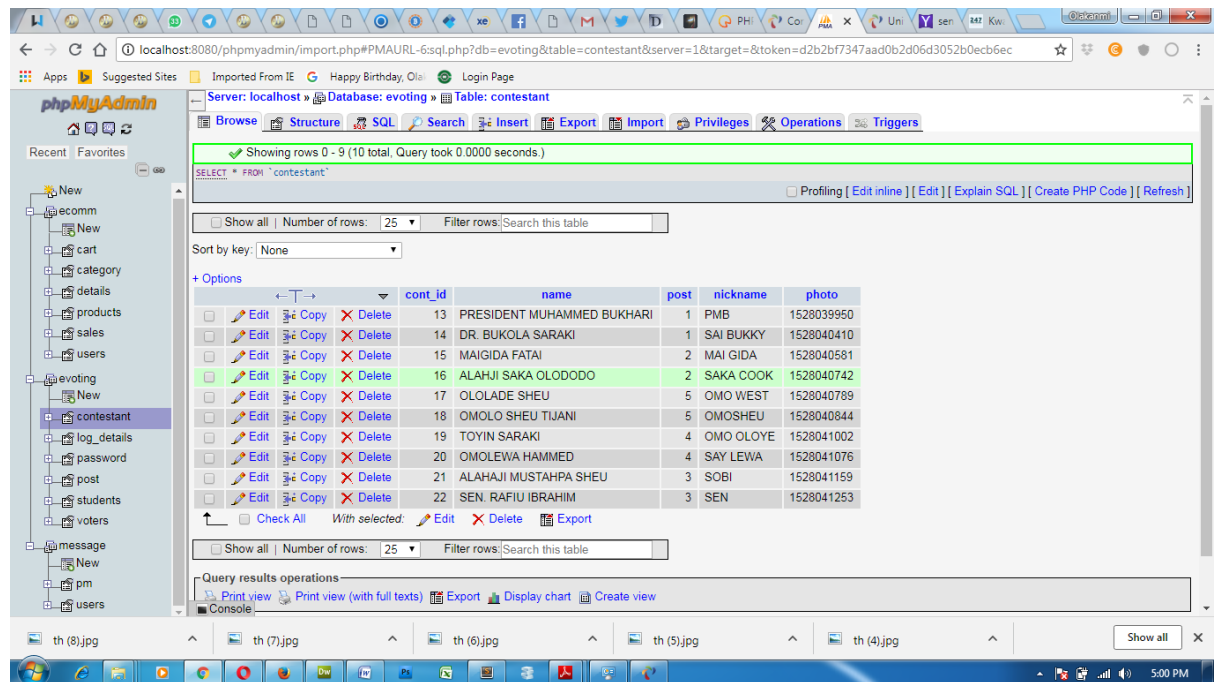


Figure 4.7 : Add Contestant

4.1.2 Database Design

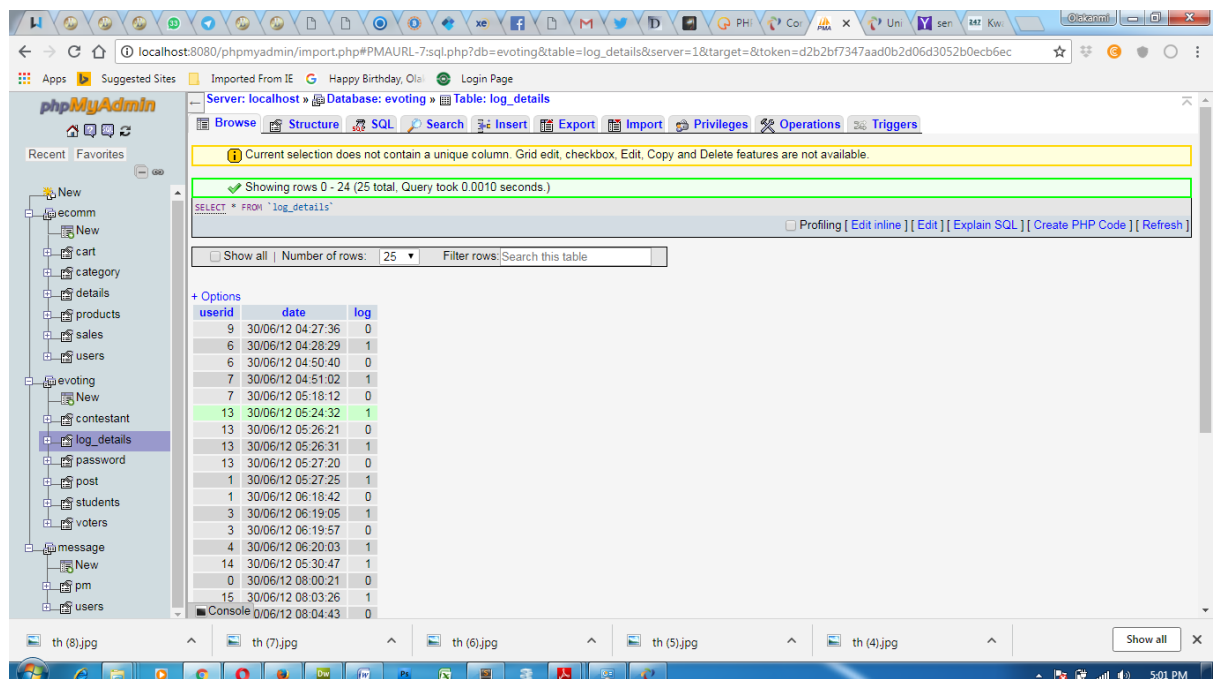
This consist of the figures of table used in the implementation of the proposed system



The screenshot shows the phpMyAdmin interface for the 'evoting' database. The 'contestant' table is selected, and its structure and data are displayed. The table has columns: cont_id, name, post, nickname, and photo. The data is as follows:

cont_id	name	post	nickname	photo
13	PRESIDENT MUHAMMED BUKHARI	1	PMB	1528039950
14	DR. BUKOLA SARAKI	1	SAI BUKKY	1528040410
15	MAIGIDA FATAI	2	MAI GIDA	1528040581
16	ALAHJI SAKA OLODODO	2	SAKA COOK	1528040742
17	OLOLADE SHEU	5	OMO WEST	1528040789
18	OMOLO SHEU TIJANI	5	OMOSHEU	1528040844
19	TOYIN SARAKI	4	OMO OLOYE	1528041002
20	OMOLEWA HAMMED	4	SAY LEWA	1528041076
21	ALAHAJI MUSTAHPA SHEU	3	SOBI	1528041159
22	SEN. RAFIU IBRAHIM	3	SEN	1528041253

Table 4.1: Contestant Table



The screenshot shows the phpMyAdmin interface for the 'evoting' database. The 'log_details' table is selected, and its structure and data are displayed. The table has columns: userid, date, and log. The data is as follows:

userid	date	log
9	30/06/12 04:27:36	0
6	30/06/12 04:28:29	1
6	30/06/12 04:50:40	0
7	30/06/12 04:51:02	1
7	30/06/12 05:18:12	0
13	30/06/12 05:24:32	1
13	30/06/12 05:26:21	0
13	30/06/12 05:26:31	1
13	30/06/12 05:27:20	0
1	30/06/12 05:27:25	1
1	30/06/12 06:18:42	0
3	30/06/12 06:19:05	1
3	30/06/12 06:19:57	0
4	30/06/12 06:20:03	1
14	30/06/12 05:30:47	1
0	30/06/12 08:00:21	0
15	30/06/12 08:03:26	1
0	30/06/12 08:04:43	0

Table 4.2: Duration of User Log in Out Details

Showing rows 0 - 4 (5 total. Query took 0.0010 seconds.)

```
SELECT * FROM `post`
```

Number of rows: 25

Sort by key: None

	id	postname
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	1	President
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	2	Governor
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	3	Senator
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	4	House of Representative
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	5	Chairman

Check All With selected: ☐ Edit ☐ Delete ☐ Export

Number of rows: 25

Query results operations: [Print view](#) [Print view \(with full texts\)](#) [Export](#) [Display chart](#) [Create view](#)

Table 4.3: Post Table

Showing rows 0 - 14 (15 total. Query took 0.0000 seconds.)

```
SELECT * FROM `students`
```

Number of rows: 25

Sort by key: None

	id	matric_no	password	status
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	1	10/52ha109	ola	1
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	2	10/52ha110	welcome	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	3	09/52ha001	olajide	1
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	4	09/52ha002	kasali	1
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	5	09/52ha003	jacob	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	6	09/52hy001	mathew	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	7	09/52hp004	oladele	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	8	09/52hn010	Rufai	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	9	10/52ha115	Raheem	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	10	09/52ha102	Udeaja	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	11	09/52hn009	adewale	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	12	nd/07/com/088	waslam	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	13	HND/08/STA/223	1234	0
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	14	08/52HA048	HARUN	1
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	15	07/52ha154	abiodun	1

Table 4.4: Voter's Table

4.1.3 Procedure Design

This refers to the step by step method of using the proposed system. The proposed system comprises of Add a Voter Details, Add Post, Add Contestant, View result, List of Contestant, Voted User, Not Yet Voted User, All Voters. The steps to use the proposed system are as follows

- a) On the address bar of any browser type <http://localhost/evoting/index.php>
- b) You are prompted to supply the username and password this verifies that you are a registered voter and has the privileged to vote.
- c) If the username and password supplied are correct as that of the voter you are prompted with the home page with the list of contestant based on their post and with their picture and at the end you click on submit to validate your votes.
- d) The username and password are in two formats as an administrator as well as a user.
- e) As an administrator you are to type <http://localhost/evoting/admin/index.php> on the address bar.
- f) As an administrator you are prompted with the administrator page where the back end of the voting exercise is carried out.

4.2 Implementation of the System

4.2.0 Choice of Programming Language

The reason for choosing PHP is that it is among the language of the web and as well it is an open source language in which help is readily available when needed and its level of pedagogy.

Advantages of PHP

The following are the advantages of using PHP

1. **Learning curve** –PHP is a very easy learning curve unlike Java or Perl. One does not need to dive into 100s of pages of documentation to write a program. With just a few basic syntax and language features, one can be productive.

Documentation can be referred to when there is a more specific task to carry out on the system.

2. **Database Integration** – PHP can be compiled with functions to interact with lot of database. PHP with My SQL is a very popular combination.
3. **Object Oriented Programming** – PHP provides support for classes and objects. Support for object oriented programming is sufficient enough for most programming tasks related to the web. PHP supports constructors, derived classes etc.
5. **Scalability** – Traditionally, interactive web page is achieved using CGI programs. CGI programs do not scale well, because, each run of a program occurs as a separate process. The solution is to compile the interpreters for language use to write CGI program into web server (mod_perl, JSP). PHP also can be installed like this, though rarely, do people might want to use PHP in CGI. Embedded PHP installations scale well.

2.2.1 Hardware Support

CPU	:	PENTIUM IV
PROCESSOR SPEED	:	2 GHz
COPROCESSOR	:	BUILT IN
TOTAL RAM	:	1GB or Higher
HARD DISK	:	80 GB
KEYBOARD	:	105 KEYS
MOUSE	:	LOGITECH MOUSE
DISPLAY	:	SGVA COLOR

2.2.2 Software Support

The proposed system makes use of;

- i. Macromedia fireworks for graphics work on the images and background used in the system,

- ii. macromedia Dream weaver (a text editor) while;
- iii. MY SQL is used as the database.

4.1.1 Implementation Techniques Used In Detail

The implementation technique to be use in the system is parallels, a system that support the current system along-side with the proposed system. This means that to adopt the proposed system a paper and pen method that is currently in used will still be in existence so that a failure in the proposed system will not lead to total loss of applicants.

4.3 Documentation of the System

4.3.1 Program Documentation

Administrator Environment: The administrator environment entails the following

- a) Add a Voter Detail
 - b) Add Contestant
 - c) View Result
 - d) List of Contestant
 - e) Voted User
 - f) Not Voted User
 - g) Registered Voter
- a) Add Voter Detail: This page allows the accredited voter details to be added to the database and this allows the registered user to be able to log in and vote in the voter's environment.
 - b) Add Contestant: It allows the list of contestant who has gotten the form and submitted to be added to the database with their details. This include their pictures and nicknames together with the pot aspired for.
 - c) View Result: Result of the election can be viewed and not able to be edited by the administrator to avoid biasness and all other forms of the problems which arise from the traditional voting system. The result is grouped in the order of the post displaying the score of each candidate immediately after their names.

- d) List of Contestant: This displays the list of previously added contestant with equivalent post applied for.
- e) Voted User: It displays the list of user who has voted in the on going voting exercise.
- f) Not Voted User: This displays the list of user who has not voted in the on going exercise
- g) All Voters: This displays the list of all registered voter for the election.

Voters Environment

The voters' environment prompts the user to supply the previously saved fingerprint for comparison with the user supplied fingerprint. If there is a match between the supplied fingerprint and the user has not yet voted then the voting environment will be displayed for the user to vote otherwise if the user has voted a message is displayed for the user.

4.3.2 Operating the System

In order for the proposed system to be used on any computer system it takes the following ways

- I. Boot the system
- II. Copy the folder to www inside wamp folder of the drive C: after WAMP server is installed onto the system.
- III. Open any browser on the system (Microsoft internet Explorer, Mozilla Firefox, Netscape Navigator, Opera, Flock, Safari e.t.c)
- IV. Type <http://localhost/evoting/index.php> on the address bar and press the return key or enter key.

4.3.2 Maintaining the System

System maintenance is a critical aspect of ensuring the long-term effectiveness, security, and usability of the developed web-based voting platform. Given that the

system integrates advanced cryptographic protocols such as Zero-Knowledge Proofs (ZKPs), maintaining it requires specialized oversight to address both routine and complex challenges that may arise post-deployment.

First and foremost, regular software updates are essential to patch security vulnerabilities, upgrade cryptographic libraries, and incorporate performance improvements. As cryptographic standards evolve and new attack vectors are discovered, especially in areas like zero-knowledge systems, it is vital that the system's encryption and verification modules are kept up-to-date with the latest best practices and proven algorithms.

Secondly, database maintenance is required to ensure the integrity and availability of voting records and system logs. Routine database backups and consistency checks help to prevent data corruption or loss, particularly in the event of unexpected system failures or cyberattacks. It is also important to enforce strict access control to the database through role-based authentication mechanisms to avoid insider threats.

Furthermore, user support and interface enhancements form part of ongoing maintenance. As feedback is gathered from users, especially during pilot elections or public usage, updates to the user interface may be necessary to enhance usability and accommodate users with different levels of digital literacy. Bug fixes and compatibility updates (e.g., with modern web browsers and mobile devices) should also be regularly deployed.

The system must also be monitored continuously for potential cybersecurity threats. Real-time logging, intrusion detection systems, and anomaly detection mechanisms should be implemented to detect and respond to unauthorized activities swiftly. Maintenance personnel should conduct periodic security audits and penetration testing to assess the system's resilience and make necessary adjustments.

Additionally, maintaining the system requires legal and compliance reviews, especially in electoral environments governed by national laws or international

standards. Any updates or modifications to the system should be reviewed to ensure they align with electoral commission guidelines, data protection regulations, and the principles of free and fair elections. In conclusion, maintaining the proposed web-based voting system is a continuous, multidimensional process involving technical updates, cybersecurity vigilance, user-centered enhancements, and compliance oversight. A well-structured maintenance strategy will ensure the platform remains reliable, secure, and trusted by all election stakeholders over time.

Chapter Five

Summary, Conclusion and Recommendation

5.1 Summary

This research project was undertaken to design and implement an improved web-based voting system that leverages Zero-Knowledge Proof (ZKP) encryption to overcome the limitations of traditional e-voting platforms. The motivation stemmed from the critical need for systems that ensure voter privacy, election integrity, and transparency while remaining accessible to a broad range of users. The study commenced with an examination of existing voting systems and their vulnerabilities, including inadequate privacy, poor verifiability, and exposure to cyberattacks. The literature review identified Zero-Knowledge Proofs—specifically zk-SNARKs and zk-STARKs as a promising solution for ensuring that votes can be verified without disclosing vote content.

The proposed system was developed using modern web technologies with an integrated ZKP cryptographic layer. The architecture included modules for user registration, vote casting, proof generation, verification, and result tallying. Security testing, functional testing, and user acceptance evaluation were carried out to validate the system's efficiency and robustness. The test results confirmed that the system successfully ensures voter anonymity, prevents vote tampering, and provides a transparent yet secure voting process. In addition, the system interface was designed for ease of use, enabling even non-technical users to vote securely and confidently.

5.2 Conclusion

This study concludes that Zero-Knowledge Proof encryption can significantly enhance the security and privacy of web-based voting systems. By applying ZKP protocols, the system enables voters to prove the legitimacy of their votes without revealing any sensitive information, solving one of the most pressing challenges in digital elections. The successful implementation of this system demonstrates that it is possible to create a platform that is secure, verifiable, and usable for both small- and

large-scale elections. It also proves that end-to-end verifiability and user anonymity are not mutually exclusive, but rather achievable through the thoughtful integration of cryptographic techniques.

Furthermore, the system's web-based design increases accessibility for remote and diasporic voters while reducing operational costs and election timelines. The outcomes of this research contribute to the body of knowledge on digital trust, secure communications, and cryptographic applications in e-governance. Most importantly, it opens the door for wider adoption of advanced cryptographic voting methods in democratic societies, especially in developing countries where electoral malpractice is prevalent.

5.3 Recommendation

Based on the findings and success of the proposed system, several recommendations are made. Firstly, governments and electoral bodies should consider investing in secure cryptographic voting technologies like ZKP-based systems to enhance electoral transparency and trust. While the technology is relatively complex, integrating it with user-friendly interfaces as demonstrated in this study—can ensure mass adoption without requiring voters to understand the underlying cryptography.

Secondly, further research should be conducted into optimizing Zero-Knowledge Proof algorithms for faster performance and lower computational costs, especially for deployment in resource-constrained environments. This will make the technology more scalable and applicable to real-world national elections.

Thirdly, future implementations should include biometric authentication and blockchain integration to strengthen identity verification and tamper resistance. Combining ZKPs with distributed ledger technology may create a holistic solution that is not only private and verifiable but also immutable and decentralized.

Finally, policy frameworks and legal backing should be established to support the deployment of such digital voting systems. Adequate digital literacy campaigns

and public sensitization are essential to build trust in the use of advanced voting technologies.

REFERENCES

- Adekunle I. O., Adekunle A. E. and Tajudeen A. A. (2013). "A Comparative Study of Synchronous And Blended Online Learning System Resources". International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 11.
- Alonso F., López G., Manrique D. and Viñes J. M. (2015). "An instructional model for web based e-learning education with a blended learning process approach". British Journal of Educational Technology, 36(2), 217-235.
- Brandon H. (2019). "E-learning". A research note by Namahn, found in: www.namahn.com/resources/.../note-e-learning.pdf, Retrieved on 05/12/2017
- Gilhooly K. (2019). "Making e-learning effective". Computerworld 35 (29): 52– 53.
- Iqrar A. and Bokhari M. U. (2013). "The Combine Effect of Synchronous and Blended Online Learning System on Distance Education". IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814 www.IJCSI.org
- Jereb E. and Šmitek B. (2016). "Applying multimedia instruction in e-learning". Innovations in Education and Teaching International, 43(1), 15- 27.
- Koohang A., and Harman K. (2015). "Open source: A metaphor for e-learning". Informing Science Journal, 8, 75-86.
- Oye N.D., Mazleena S. and Iahad N. A. (2012); "E-Learning Methodologies and Tools". International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No.2.
- Paily M. U. (2015). "Instructional Design in E-learning". Unit in the course on Educational Communication Technologies for IGNOU's MA in Distance Education. IGNOU: New Delhi
- Roberta G. (2016). "A brief history of elearning (infographic)". <https://www.efrontlearning.com/blog/2013/08/a-brief-history-of-elearninginfographic.html>
- Shaik M. J. (2012). "E-Learning: Strategies for Delivering Knowledge in the Digital Age" McGraw-Hill.
- Wai A. and Sharma K. (2015). "E-Learning New Trends and Innovations". Deep and Deep Publications Private Ltd., New Delhi, 2005

Szabo M. and Flesher K. (2018). "CMI Theory and Practice: Historical Roots of Learning Management Systems". Proceedings of World Conference on E- Learning in Corporate, Government, Healthcare, and Higher Education 2002 (White Paper) (Montreal, Canada: In M. Driscoll and T. Reeves (Eds.)): pp. 929–936. ISBN 1-880094-46-0.