ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/389319396

Smart Voting System

Book · December 2024

CITATIONS
0

READS
268

4 authors, including:

Rehan Raja
Integral University
31 PUBLICATIONS **98** CITATIONS
SEE PROFILE

Kasi Vinayakan
Khadir Mohideen College
34 PUBLICATIONS **647** CITATIONS
SEE PROFILE

Vasuki Murugesan
Srinivasan College of Arts and Science
132 PUBLICATIONS **2,494** CITATIONS
SEE PROFILE

All content following this page was uploaded by Prof A. Dinesh Kumar on 25 February 2025.

The user has requested enhancement of the downloaded file.

smart
VOTING SYSTEM

R. Raja
M. Vasuki
K. Vinayakan
A. Dinesh Kumar

Smart Voting System

R. Raja
K. Vinayakan
M. Vasuki
A. Dinesh Kumar

DK International Research Foundation

Imprint:
Any brand names and product names mentioned in this book are subject to trademark, brand or patent protection and are trademarks or registered trademarks of their respective holders. The use of brand names, product names, common names, trade names, product descriptions etc. even without a particular marking in this work is in no way to be construed to mean that such names may be regarded as unrestricted in respect of trademark and brand protection legislation and could thus be used by anyone.

Publisher & Printers:
DK International Research Foundation, Perambalur, Tamil Nadu, India
Email: dkirfceo@gmail.com / Phone: +91 95 00 77 99 68
Website: www.dkirf.org

ISBN: 978-93-90956-90-6

ISBN Supported By: Raja Rammohun Roy National Agency for ISBN, Department of Higher Education, Ministry of Education, Government of India
www.isbn.gov.in

No. of Pages: 110
Date of Publication: December 2024

Cite the Book: R Raja, K Vinayakan, M Vasuki, AD Kumar, Smart Voting System, DK International Research Foundation, ISBN: 978-93-90956-90-6, December 2024

Copyright @ 2024, DK International Research Foundation, Perambalur, Tamil Nadu, India

To Reach the Authors:
- R. Raja, Email: nsraja1984@gmail.com
- K. Vinayakan, Email: k.vinayakan@gmail.com
- M. Vasuki, Email: vasuki.scas@gmail.com
- A. Dinesh Kumar, Email: dradineshkumar@gmail.com

Smart Voting System

By

Dr. R. Raja

Department of CSE (CS), CVR College of Engineering, Vastunagar, Mangalpalli, Ibrahimpatnam, Rangareddy, Telangana, India

Dr. K. Vinayakan

Khadir Mohideen College (Affiliated to Bharathidasan University), Adirampattinam, Thanjavur, Tamil Nadu, India

Dr. M. Vasuki

Srinivasan College of Arts and Science (Affiliated to Bharathidasan University), Perambalur, Tamil Nadu, India

Dr. A. Dinesh Kumar

Khadir Mohideen College (Affiliated to Bharathidasan University), Adirampattinam, Thanjavur, Tamil Nadu, India

DEDICATION

This work is dedicated to the unwavering pursuit of truth, transparency, and integrity in the democratic process. To the countless individuals who have fought and continue to fight for the right to vote, the cornerstone of democracy, this book is a testament to your struggles and triumphs. May this effort serve as a catalyst for change in how we engage with the democratic process, ensuring that future generations experience a system that is not only secure and efficient but also inclusive, transparent, and reflective of the ideals upon which democracies are built.

To those who innovate in the name of progress, pushing the boundaries of technology to safeguard our rights and freedoms, your tireless work is shaping a better future for all. This book is also dedicated to the researchers, scholars, and technologists who continue to work on the development of systems that will secure the future of electronic voting and ensure the protection of voter privacy, integrity, and access.

In memory of those who have sacrificed so much for democratic ideals, and in honor of those who will continue to do so, this work is humbly offered as a contribution to the ongoing evolution of our collective democratic experience. May this journey toward innovation in voting systems ultimately create a world where every voice is heard and every vote truly counts, no matter the barriers.

To the citizens of the world-your participation, trust, and belief in the power of voting are the foundation of a brighter, more equitable future for us all. It is with great respect for the democratic values that guide us, and the technological innovations that empower us, that this work is dedicated to all who believe in progress and equality.

This dedication is also for the dreamers who envision a future where technology serves humanity, not just as a tool for efficiency but as a safeguard for the very principles we hold dear. To those who relentlessly challenge the status quo, seeking new ways to bridge the gaps in accessibility and security, this work is a tribute to your vision and determination.

And finally, to all who place their trust in the democratic process, may we continually strive to refine it and make it as secure, inclusive, and trustworthy as it deserves to be. The future of our democracy depends on the work we do today to build systems that protect the sanctity of every individual’s vote, ensuring that the voice of the people remains strong, united, and free.

ACKNOWLEDGEMENT

We, the authors, would like to express our sincere gratitude to all those who have contributed to the completion of this book. Without the support, guidance, and expertise of numerous individuals and organizations, this research would not have been possible.

First, we would like to extend our deepest appreciation to our academic advisors and mentors, whose guidance and constructive feedback have been invaluable. Your continuous support, encouragement, and expertise have greatly shaped our work and inspired us throughout the research process.

We also wish to acknowledge the faculty and staff at CVR College of Engineering, Vastunagar, Mangalpalli, Ibrahimpatnam, Rangareddy, Telangana / Khadir Mohideen College (Affiliated to Bharathidasan University), Adirampattinam, Thanjavur, Tamil Nadu / Srinivasan College of Arts and Science (Affiliated to Bharathidasan University), Perambalur, Tamil Nadu for providing the resources and collaborative environment necessary for the successful execution of this book. The academic and technical support we received from the institution has been crucial to the development of our work.

A special thanks to the technology experts and researchers in the fields of cryptography, blockchain, and facial recognition who shared their knowledge and assisted us in overcoming technical challenges. Your insights and expertise ensured the development of a secure and reliable e-voting system.

We are also grateful to the developers and engineers who helped implement the various technological components of the system. Your dedication and collaboration were vital in making the technical vision of our project a reality.

Finally, we would like to express our heartfelt thanks to our families and friends for their unwavering support and encouragement throughout this journey. Your belief in our work has been a constant source of motivation.

To all those who contributed to this work, whether directly or indirectly, we thank you for your valuable input and support. This project is a reflection of our collective effort and commitment to advancing the field of electronic voting and democratic participation.

SUMMARY OF THE BOOK

In today's democratic landscape, the act of voting is foundational to the expression of a nation's collective will. However, traditional voting methods, primarily based on paper ballots and in-person voting, present a series of challenges. These challenges range from logistical difficulties and resource constraints to security concerns and lack of accessibility. The book proposes the development and implementation of a Smart Voting System, a modern solution to address these challenges and revolutionize the voting process in the digital age. By integrating cutting-edge technologies such as blockchain, cryptography, facial recognition, and multi-factor authentication, this book explores how an accessible, secure, and efficient online voting system can be created.

The main objective of the proposed voting system is to overcome the limitations of traditional, paper-based voting. The system enables remote voting, ensuring that individuals can cast their votes from the comfort of their homes or any location with internet access. This not only streamlines the voting process but also increases accessibility, particularly for people who face physical barriers to in-person voting, such as the elderly, disabled individuals, or those living in remote areas. By allowing votes to be cast digitally, the system aims to increase voter participation and engagement in the democratic process.

Security is a primary concern in any voting system, and the proposed Smart Voting System takes this into account by implementing multiple layers of protection. A key feature of the system is the use of facial recognition technology for voter authentication. This, combined with a robust cryptographic framework, ensures that the identity of voters is verified and that their votes are securely transmitted and stored. The system employs advanced cryptographic techniques, including zero-knowledge proofs, to preserve voter privacy and safeguard against potential fraud. The integration of these technologies guarantees the integrity of the election process, ensuring that votes are counted accurately and that voter anonymity is maintained.

Furthermore, the system's blockchain-based architecture introduces transparency and verifiability, two crucial features for building trust in the voting process. Blockchain technology ensures that each vote is recorded in a tamper-proof ledger, preventing any alteration or manipulation of vote data. This decentralized structure not only prevents fraud but also provides a transparent record of the election results, which can be audited by any interested party. The use of blockchain in electronic voting represents a significant step forward in making the voting process more secure and transparent.

Another key innovation explored in the book is the integration of multifactor authentication (MFA). By requiring voters to undergo multiple verification steps-such as facial recognition, fingerprint scanning, and the use of one-time passcodes (OTPs)-the system ensures that only eligible individuals can cast their votes. This multi-layered authentication process mitigates the risk of identity theft and voting fraud, addressing one of the primary concerns of electronic voting systems.

The book also highlights the limitations of existing electronic voting models, particularly their vulnerability to security breaches and their high operational costs. The proposed Smart Voting System tackles these issues by leveraging distributed ledger technologies and secure cryptographic protocols to enhance both security and scalability. The book explores how these innovations can help streamline the voting process, reduce costs, and improve the overall efficiency of elections.

In addition to enhancing security and accessibility, the Smart Voting System focuses on the user experience. The system's interface is designed to be intuitive and easy to use, ensuring that voters can participate in the electoral process with minimal technical knowledge. By incorporating machine learning algorithms, the system can be adapted to the needs of different voters, making the process more inclusive.

The book concludes by discussing the broader implications of adopting digital voting systems. As societies become increasingly digitized, there is a growing need for electoral systems that reflect these changes. The proposed system not only addresses the immediate challenges of traditional voting methods but also sets the stage for a more inclusive and accessible future for democratic participation. It emphasizes the potential for blockchain and cryptography to transform the electoral process, making it more secure, transparent, and trustworthy. The system ultimately aims to inspire greater public confidence in the democratic process and encourage more individuals to participate in elections, knowing that their vote will be securely counted.

In summary, the Smart Voting System proposed in this book represents a significant leap forward in the evolution of democratic governance. It combines the latest advancements in technology to create a voting system that is more secure, accessible, and transparent, ensuring that every vote counts and that the integrity of the electoral process is maintained. By modernizing the voting process, this system aims to increase voter participation, build public trust, and contribute to the creation of more inclusive and equitable democratic societies.

CONTENTS

PREFACE

In the global landscape of democracy, the importance of a fair and efficient voting system cannot be overstated. Presently, reliance on in-person voting poses challenges in operational efficiency, resource management, and timely result announcements. This project endeavors to modernize the voting experience by introducing an accessible online voting system, circumventing the limitations of physical presence. Users can cast their votes remotely via computers, streamlining the process and catering to a diverse population. To bolster security, a robust authentication process is employed, integrating facial recognition and secure hash comparison. These measures authenticate voters, mitigate identity fraud, and ensure the integrity of the voting system. In addition to fortifying security measures, the online voting system offers convenience and accessibility, particularly for individuals facing barriers to physical voting locations.

By enabling remote voting, the system promotes inclusivity and broadens participation in the democratic process. Furthermore, the integration of facial recognition technology enhances user experience and instills confidence in the authenticity of the voting process. Overall, this initiative represents a pivotal step towards a more modern, secure, and inclusive elector.

In a democratic regime, voting is crucial to making collective decisions. Unfortunately, although this activity has great significance and value, little effort has been made to improve the way we vote. Paper ballots are still the most used method, although this method is relatively simple, brings many inconveniences, and represents a contradiction to the modern world and its advances. This paper mostly focuses on a review study of blockchain-based voting systems. It aims at identifying the strategies and the guidelines as well as provides a comprehensive end-to-end electronic voting system based on blockchain, with the help of cryptographic techniques such as zero-knowledge proofs to improve privacy.

The novelty of this paper is that we tackle the limitations of electronic voting systems found in the literature, including cost, identity management, and scalability problems. Our purpose is to provide key elements for organizations on how to design their proper electronic voting system based on blockchain technology.

The system can showcase several well-known blockchain frameworks that offer blockchain as a service and a related electronic E-voting system that is based on blockchain and addresses all restrictions in multiple ways. It also maintains participant anonymity while allowing for open scrutiny. It has long been a difficulty to develop an electronic voting system for associate in nursing that complies with legislators' regulatory requirements. Within the field of information technology, distributed ledger technologies provide an interesting technological leap for associate in nursing. Blockchain technology offers a limitless range of possibilities for profiting from sharing economies. Blockchain promises to increase the robustness of electronic voting systems, making it a potentially disruptive technology of the modern era. This method offers a chance to take advantage of blockchain's advantages, such as its transparency and crypto logical underpinnings, to achieve an effective theme for electronic voting.

The proposed topic achieves end-to-end verifiability and complies with the fundamental requirements for electronic voting methods. The system offers a thorough examination of the theme, successfully demonstrating its efficacy in achieving associate in nursing end-to-end verifiable e-voting.

The primary goal of every voting system is to ensure that electorate vote counts therefore, electronic democratic governance that provides a transparent and trusted election is needed. The traditional method of voting involves the use of physical paper ballot to casts vote. This is susceptible to time wasting procedures, ballot snatching, lacks voter privacy and question the integrity of fair electoral process. This paper describes our attempt to improve

the authentication and integrity of evoting system using multifactor authentication and cryptographic hash function methods. Our system meets two of the key security issues in secured e-voting system: The threat of erring voter's authentication and integrity of vote transmitted over insecure wireless medium. The results obtained from the test and evaluation of secured electronic voting system based on this model so far shows an avenue to ensure the integrity of the electoral process and as such, encourages the populace to have trust in the election, through the detection of altered votes in wireless medium and voter authentication through One time Short Message Service (OTSMS) and Grid Card multifactor authentication.

The issue of security in Information and Communication Technology has been identified as the most critical barrier in the widespread adoption of electronic voting (e-voting). Earlier cryptographic models for secure evoting are vulnerable to attacks and existing stegano-cryptographic models can be manipulated by an eavesdropper. These shortcomings of existing models of secure e-voting are threats to confidentiality, integrity and verifiability of electronic ballot which are critical to overall success of e-democratic decision making through e-voting. This paper develops an enhanced stegano-cryptographic model for secure electronic voting system in poll-site, web and mobile voting scenarios for better citizens' participation and credible e-democratic election.

The electronic ballot was encrypted using Elliptic Curve Cryptography and Rivest-Sharma-Adleman cryptographic algorithm. The encrypted voter's ballot was scattered and hidden in the Least Significant Bit (LSB) of the cover media using information hiding attribute of modified LSB-Wavelet stegano-graphic 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).The results after quantitative performance evaluation shows that the developed stegano-cryptographic model has generic attribute of secured e-voting relevant for

the delivery of credible e-democratic decision making. The large scale implementation of the model would be useful to deliver e-voting of high electoral integrity and political trustworthiness, where genuine e-elections are conducted for the populace by government authority.

A novel hybrid design based electronic voting system is proposed, implemented and analyzed. The proposed system uses two voter verification techniques to give better results in comparison to single identification based systems. Finger print and facial recognition based methods are used for voter identification. Cross verification of a voter during an election process provides better accuracy than single parameter identification method. The facial recognition system uses Viola-Jones algorithm along with rectangular Haar feature selection method for detection and extraction of features to develop a biometric template and for feature extraction during the voting process. Cascaded machine learning based classifiers are used for comparing the features for identity verification using GPCA (Generalized Principle Component Analysis) and K-NN (K-Nearest Neighbor). It is accomplished through comparing the Eigen-vectors of the extracted features with the biometric template pre-stored in the election regulatory body database. The results of the proposed system show that the proposed cascaded design based system performs better than the systems using other classifiers or separate schemes i.e. facial or finger print based schemes. The proposed system will be highly useful for real time applications due to the reason that it has 91% accuracy under nominal light in terms of facial recognition

CHAPTER I

INTRODUCTION

Elections are inevitable happenings in a democratic society, and it is the sole responsibility of both the government and the citizens to make sure that it happens in a safe and secure way and also it takes place smoothly. However, the current voting system, reliant on in-person voting, poses challenges in terms of efficiency and accessibility. With the need for a more streamlined and inclusive approach, this project seeks to revolutionize the voting system by introducing a remote voting mechanism. This shift aims to overcome the limitations of the traditional method, reducing the reliance on extensive manpower and expediting the election result announcement process.

The proposed system addresses the current inefficiencies by allowing citizens to exercise their voting rights remotely, leveraging the convenience of digital platforms. This transition not only enhances accessibility but also encourages broader participation, particularly among individuals who may face geographical or physical constraints. By enabling voters to cast their ballots from the comfort of their computers, the project endeavours to usher in a new era of efficiency and flexibility in the Indian electoral landscape.

One of the project's key innovations is the implementation of a robust two-step authentication process, ensuring the utmost security and integrity of the remote voting system. The first step involves cutting-edge face recognition technology, a modern authentication approach that verifies the legitimacy of the user attempting to vote. The second step employs a secure hash comparison of the voter ID and password, adding an extra layer of protection to prevent unauthorized access and uphold the sanctity of the voting process. This multi-tiered authentication system is designed to instil trust in the remote voting system,

assuring citizens of the reliability and security of their digital participation in the democratic process.

Go to the polls (or voting) is one of the cornerstones of modern democracy. It enables people to actively participate in decision-making by choosing their representatives among several candidates who will be mandated to act fairly act on their behalf. Even though voting is fundamental, it has changed little over time, and we still have paper-based methods as the most common voting method. The paper-based method has its pros, such as ease of use and protection of voter privacy, which explain the persistence in adoption for decades. However, most countries still rely on paper ballots to cast votes. In a paper ballot voting system, voters prove their identities with their ID cards at a voting station to get access to the voting booth; they then get to vote for their delegate in the paper ballot, fold the ballot, and put it into the ballot box. When the election operation is over, the ballot boxes are collected and then transferred to the tallying station where they are unlocked and unloaded of ballots. The ballots are then manually examined, and the votes are counted, as shown in figure 1.1.

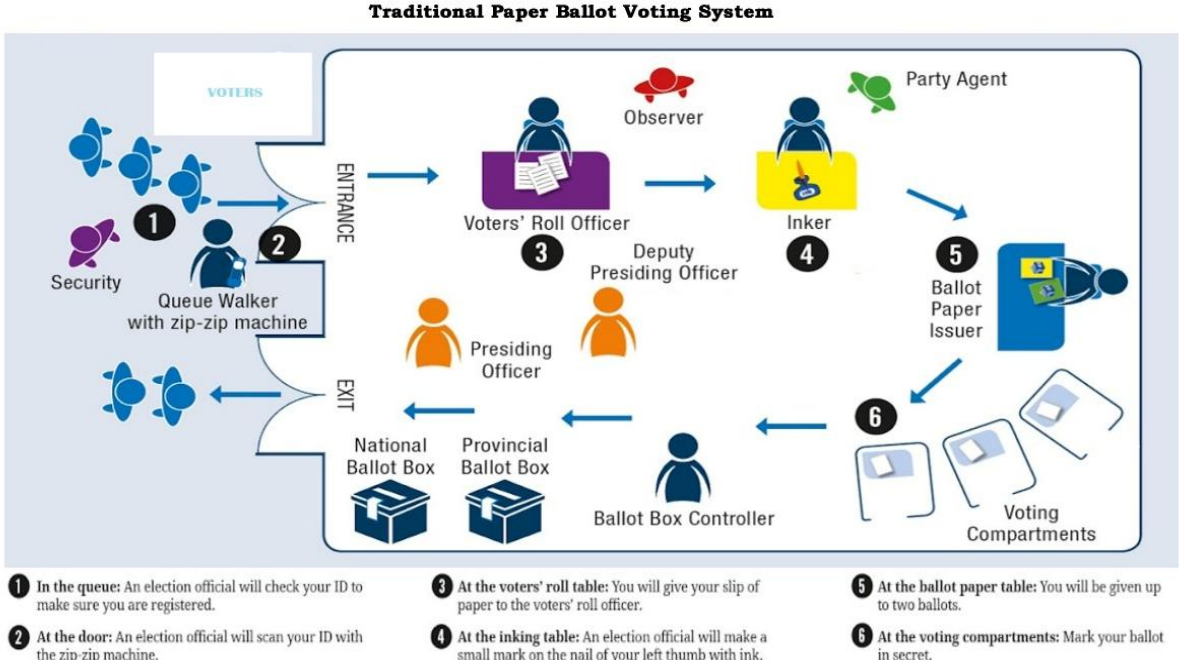


Figure 1.1: Traditional paper ballot voting system.

The traditional paper ballot voting method presents some advantages, mainly the facility of use, even for illiterate people, and the secrecy of the vote, since the ballot is not linked in any way to the voter. Moreover, it has many disadvantages. The current challenges and drawbacks of traditional paper-based voting systems are the following.

- Cost issues: Logistics expenses that include tons of papers, transportation, polling stations, and human labour.
- Accessibility issues: Most paper voting systems require a trip to the polling stations. This dependency can be a struggle for people living in remote areas, citizens residing abroad, or people with disabilities.
- Integrity issues: Since people manage the system, it is at risk of corruption and human errors. It is strongly dependent on the efficiency and trustworthiness of people.
- Inefficiency issues: Running a national election is a huge project, and projects at that scale tend to go wrong. This traditional system takes a lot of time and money to implement and manage. The paper ballots are not faulted tolerant, many ballots are not valid and hence not counted, and therefore wasted.

Another voting method is electronic voting, it can be in the form of a voting machine in a process like paper voting but instead of paper, voters cast their vote via machines found in polling stations. Alternatively, it can be done online; voters cast their votes using their electronic devices. The election results are automatically counted; as a result, electronic voting is faster and more convenient than the traditional voting system. It has numerous issues. There is no guarantee that the voters' vote choice is not leaked or manipulated. Most electronic systems are black boxes and impossible to audit and are also centralized, which puts them at risk of denial-of-service attacks. We believe that for an electronic system online to be efficient for a large-scale election, it must possess the following properties:

- Security: Like any online public system, it should be immune to different cyber-attacks.
- Integrity: Only verified and eligible voters can vote and only once (a double spending problem in the context of blockchain), once the vote is cast, it cannot be altered.
- Accessibility and availability: Eligible voters should be fit to access the system remotely from anywhere and during the entire voting time.
- Privacy: The voter's private information should be secure and protected while voting should be done anonymously. The system of voting shall not reveal who voted for whom (ballot secrecy).
- Transparency: Overall system must be auditable by the public. It should not be a black box where nobody knows how to operate.
- End-to-end or E2E verifiable: Voters should be able to verify from end-to-end the cast (cast-as-intended) and the record (recorded-as-cast) of their vote as well as its tally (tallied-as-recorded) without being able to prove the choice to others (receipt freeness).
- Affordability: The cost to implement and maintain the system should be reasonable and less expensive than traditional systems.
- Scalability: The system must handle a large-scale election in terms of the number of participants and the response time.
- Coercion resistance: Voters should not be able to share or prove their vote choice with a coercer, to protect voters from blackmailing or being bought (vote buying), so the results of the election cannot be influenced unlawfully.

Blockchain systems can be the missing puzzle to solve most of these cons while maintaining maximum security. Blockchain is an open-source technology, therefore transparent and auditable [1]. This article is an extension of our previous published papers

[2, 3]. In Fatrah et al.'s [2] study, we explored the feasibility of a blockchain-based voting system. Moreover, in Fatrah et al.'s [3] study, we created our first version of the system. In this paper, we are going to tackle the limitations found. In the previous articles, we assumed the existence of a user management application that the authorities use to verify the identity proof provided by the voters and also assumed that the application is secure to protect and ensure the voter data. We also found a huge scalability issue related to the cost and time, the blockchain system we designed was based on Ethereum and it turned out to be very expensive for national elections even though we had some off-chain components, also the scalability related to the time needed for the system to process all the transactions.

The preservation of an election may be a national security concern in any democracy. For the past ten years, the science of computer security has investigated the likelihood of electronic voting systems to reduce the cost of holding a national election while simultaneously meeting and strengthening election security requirements. Pen and paper have been the foundation of the legal system since the beginning of democratic candidate elections. To reduce fraud, switching from the traditional pen and paper election process to a new one that is traceable and verifiable is crucial. The protection community sees electronic choice machines as flawed since they only take physical security into account. Anybody who has physical access to such a device can tamper with it to move all votes up the stated device. A distributed, public, irreversible, and unchangeable ledger may be called a blockchain.

There are four primary ways that this new technology functions:

- The ledger can be found in several places: No single point of failure exists when it comes to distributed ledger maintenance.
- New transactions are added to the ledger by the United Nations organization, which has distributed management.

- To avoid tampering with the integrity of earlier entries, every proposed "new block" to the ledger should have reference to the earlier version of the ledger. This creates a chain that is immutable from the point at which the blockchain receives its name.
- Before a proposed new block of records is permanently added to the ledger, a consensus must be reached by the majority of the network nodes.

These technical solutions function using sophisticated encryption, offering a level of security that is on par with or greater than any previously noteworthy data. As a result, many people, including those in America, believe that blockchain technology is the greatest instrument for implementing the newest, hippie democratic voting process. This study assesses the use of blockchain technology as a service for implementing associate degree electronic voting system. The system makes the subsequent original contributions:

- Examine current blockchain frameworks that are appropriate for building blockchain-based electronic voting systems.
- Propose a blockchain-based electronic voting system that modifies liquid democracy through the usage of "permissioned blockchain" [4]

1.1 Motivation:

This research is motivated by a dedication to revolutionizing the traditional voting process and making it more accessible and secure. Recognizing the challenges inherent in conventional voting systems, including concerns about security and limited accessibility, we aim to leverage technology to create a solution that addresses these issues head-on. The overarching vision is to empower citizens by incorporating innovative technologies like facial recognition, offering a more secure and efficient means for them to exercise their democratic rights.

The driving force behind our project lies in the belief that technology can be a force for positive change in the electoral landscape. The persistent issues faced by traditional voting

methods, ranging from security vulnerabilities to geographical limitations, have spurred our commitment to developing a solution that utilizes online voting. Our motivation stems from the conviction that every eligible voter should have the opportunity to contribute to their community and nation without unnecessary impediments, fostering a more inclusive democratic process.

Furthermore, our project is motivated by a forward-looking perspective on the role of technology in democracy. Embracing the digital age, we strive to create an adaptable and resilient electoral system that aligns with the evolving needs of modern societies. By harnessing technological advancements like facial recognition, we aim to provide a more secure and efficient voting experience, ultimately contributing to a democratic process that is responsive, trustworthy, and reflective of contemporary values.

Incorporating facial recognition technology specifically addresses the imperative to enhance the security of online voting. Overall, our project's motivation is rooted in a multifaceted approach, encompassing accessibility, security, and the evolution of democracy in the digital age. Through the thoughtful integration of technology, particularly facial recognition, we aspire to contribute to a more inclusive, secure, and resilient democratic process that meets the needs of contemporary society.

1.2 Problem Statement:

Our initiative is a direct response to the inherent inefficiencies and vulnerabilities present in traditional manual voting systems. The long queues experienced at polling stations contribute to frustration and discourage potential voters, highlighting the urgent need for a more streamlined and accessible solution. Furthermore, the manual nature of these processes introduces the risk of inaccuracies and potential fraud, posing a significant threat to the credibility of the entire electoral process.

To address these challenges, our focus is on developing an innovative online voting platform that leverages advanced facial recognition technology. This approach ensures that only authorized individuals can participate, substantially mitigating the risks associated with identity fraud and unauthorized voting. Our primary goal is to enhance accessibility, allowing citizens to cast their votes remotely from any location with internet access. This inclusive approach benefits individuals facing challenges such as mobility limitations, demanding work schedules, or residing in remote areas.

In essence, our project goes beyond modernizing the voting experience; it is about reinforcing the core principles of democracy. Through the streamlining of the voting process, the implementation of robust security measures, and the promotion of inclusivity, we aim to create a voting system where every voice is heard, and every vote contributes to shaping the future of our society. Our endeavour is driven by the belief that a more accessible, secure, and inclusive electoral process is fundamental to preserving the democratic values that underpin our society.

As we envision a future where technology serves as a catalyst for positive change, we remain committed to breaking down barriers and providing a democratic experience that truly reflects the diverse needs and circumstances of our citizens. Our motivation is rooted in the transformative potential of this project, as we seek to usher in an era where the democratic process is not only more efficient and secure but also more accessible and participatory for all.

The voting system that is hereby conceived must satisfy the following requirements:

- The election system must be openly verifiable and transparent.
- The election system must ensure that the vote cast by the voter has been recorded.
- Only eligible voters must be allowed to vote.
- The election system should be tamper-proof.

- No power-hungry organization must be able to manipulate and rig the election process.

Using a Blockchain, the most important requirements are satisfied:

- Authentication: Only registered voters will be allowed to vote.
- Anonymity: The system prevents any interaction between the votes casted by the voters and their identities.
- Accuracy: Votes once cast are permanently recorded and cannot be modified or changed under any circumstances.
- Verifiability: The system will be verifiable such that the number of votes is accounted for.[6]

1.3 Objectives:

- Implementing an online voting system: Develop a user-friendly platform that enables voters to cast their votes remotely using the internet, ensuring inclusivity and ease of use.
- Integrating facial recognition technology: Incorporate a robust facial recognition feature that not only verifies the identity of voters enhancing accuracy and reliability.
- Developing a location-free voting system: Enable voters who face mobility challenges or reside in remote areas to seamlessly participate in the voting process from anywhere, fostering a more inclusive and accessible electoral system.
- Restricting access to verified voters: Implement multi-layered verification processes, including biometric data and unique identifiers, to ensure that only eligible and registered voters gain access to the online voting system, bolstering security measures.
- Facilitating candidate selection: Provide voters with comprehensive information about candidates, including their profiles, policies, and past performances, to empower them in making well-informed choices and contributing to an informed electorate.

- Establishing a Feedback Mechanism: Creating a structured feedback system will allow citizens to share their experiences and concerns, facilitating continuous improvement and refinement of the online voting platform based on user input.
- Collaborating with Election Authorities: Our project aims to collaborate with electoral bodies to ensure compliance with legal standards and regulations. This partnership ensures that our online voting system adheres to established electoral guidelines and security protocols, fostering trust and credibility.

1.4 Report Organizations:

The second chapter delves into existing literature and previous works relevant to our application, highlighting the distinctions between them and our proposed solution. It provides a comprehensive overview of the landscape, demonstrating how our application stands out in terms of functionality, design, and innovation. In the third chapter, we outline the state-of-the-art electronic voting, along with a detailed enumeration of the functional requirements it must fulfill. This section serves as a foundational guide for the development team, ensuring clarity and alignment regarding the essential components and capabilities of the application.

Moving forward to the fourth chapter, we elucidate the methodologies and strategies employed to meet the identified functional requirements. Additionally, we discuss the technology stack utilized in the implementation process. This segment is complemented by a series of UML diagrams, providing visual aids to comprehend the architectural design and structural aspects of the application.

The subsequent fifth chapter provides a Blockchain-based electronic voting system incorporating cryptographic methods. The simple rationalization could be a ‘chain’ of blocks. A block is associate degree mass set of information. knowledge square measure collected and method to suit in an exceedingly block through a process known as mining. every block may be known employing a science hash (also referred to as a digital fingerprint). The block

shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block. during this method, all the information may be connected via a connected list structure.

The sixth chapter provides E-Voting System Using Multifactor Authentication and Cryptographic Hash Functions. The purpose of system design is to create a technical solution that satisfies the functional requirements for the system. The functional specification produced during system requirements analysis is transformed into a physical architecture through system modeling and database design.

The seventh chapter provides Enhanced Stegano-Cryptographic Model for Secure Electronic Voting. The notion of security in social information systems like e-voting is correlated to critical aspects of voters and ballot confidentiality, ballot integrity, voters' authenticity and voting service availability. An e-voting system is said to be unsecured, if an attacker can exploit vulnerability (a weakness) in any phase of electioneering process. To avert insecurity in e-voting systems, researchers have formulated various steganographic techniques, cryptographic techniques and combination of both to block threats through implementation of appropriate counter measures.

The eight chapter provides A Novel Hybrid Biometric Electronic Voting System. A microcontroller can be defined as an integrated circuit that contains a core processor and memory. Microcontroller is also known as an embedded system, capable of storing, processing and transferring data and information between various peripherals interfaced with it on some logic, i.e. like a coordinating body of a circuit. With the advancement in the field of electronic technology especially in microelectronics and embedded system development, various development boards are available. These boards include Arduino-UNO, Texas Instruments MSP 430 Launchpad, Nanode, Pinguino PIC 32, Teensy 2.0, Raspberry Pi and many others.

CHAPTER II

LITERATURE SURVEY

2.1 Existing Work:

The "Secured Voting System Using Aadhar" by B. Madhuri [1], the paper proposes a comprehensive solution to address the vulnerabilities in the current voting system in India. The primary focus is on leveraging Aadhar-based authentication, incorporating biometric data such as fingerprints, to ensure the legitimacy of voters and eliminate the risk of tampering and manipulation. The system introduces a dual approach, covering in-person voting with biometric verification linked to Aadhar cards and app-based voting for migrants, further expanding the voting base. By replacing the traditional voter ID with Aadhar authentication, the proposed system aims to enhance security, prevent illegal voting, and significantly increase the overall voting percentage. The use of OTP in the app-based voting ensures a secure and accessible method for migrants to cast their votes, contributing to the digitalization of the voting process in India.

Key Features:

- The system's foundation lies in Aadhar cards, establishing a direct connection with voters by integrating their biometric data, particularly fingerprints. This meticulous process ensures a robust and authentic voter verification, reinforcing the system's commitment to electoral integrity.
- For in-person voting, the system adopts biometric verification, minimizing the risk of tampering and guaranteeing a secure and authenticated voting experience. This approach instills confidence in the electoral process, fostering a sense of trust and transparency in the overall outcomes.
- To address the voting concerns of migrants, the system introduces a dedicated mobile app. This app facilitates remote voting for migrants, employing both Aadhar

authentication and a secure One-Time-Password (OTP) mechanism. By combining these layers of security, the system ensures the inclusivity of a broader demographic, particularly those physically distant from conventional voting locations.

- The system ambitiously aspires to achieve 100% tamper-free votes, implementing stringent Aadhar-based authentication measures. This commitment underscores the system's dedication to eliminating potential manipulation, fostering a voting environment characterized by trust and transparency.
- In a strategic move, the system targets the active inclusion of migrants in the electoral process to bolster the overall voting percentage in the country. This initiative aims to reverse the declining trend in voter turnout, fostering a more representative and participatory democracy.
- Compared to traditional Electronic Voting Machines (EVMs), the proposed system is positioned as a cost-effective and scalable alternative. This economic efficiency, coupled with enhanced scalability, underscores the system's practical and sustainable solution for electoral processes in the country.
- The system's alignment with the Digital India initiative is evident in its integration of secure technology into the voting process. This forward-thinking approach not only addresses contemporary challenges but also contributes to the broader national vision of building a digitally empowered society.

The “Centralized Electronic Voting System” by Prachi Zalte [2], the paper underscores the necessity for a Centralized Electronic Voting System in India, given the heightened awareness of voting and challenges associated with traditional methods. The proposed system focuses on elevating security, efficiency, and accessibility in the voting process. By incorporating biometric authentication and Aadhaar card integration, it aims to enhance security. The transition to a web-based platform improves efficiency, enabling voters to

securely cast their ballots from any location, addressing logistical challenges and potentially boosting overall voter turnout. In essence, the Centralized Electronic Voting System seeks to overcome traditional limitations, offering a more secure, efficient, and accessible voting experience for India's diverse and expanding electorate.

Key Features:

- Fingerprint scanning is implemented for voter authentication, minimizing the risk of dummy votes.
- Aadhaar card numbers serve as user login credentials, and fingerprint data is cross-referenced with images from the Aadhaar card database for additional verification.
- The system facilitates secure remote voting, eliminating the necessity for physical voting booths and providing convenience for voters to cast their ballots from any location.
- By encouraging voter participation through a user-friendly and location-independent method, the system aims to contribute to a higher overall percentage of voter turnout.
- Enhancing upon existing voting methods, the system ensures accuracy, convenience, flexibility, privacy, verifiability, and mobility in the voting process.
- The Election Commission of India maintains a centralized database, ensuring secure storage and efficient management of voter details for the voting system.
- The proposed system reduces costs associated with traditional voting methods, such as paper-based voting, and streamlines processes like voter registration and vote counting, saving time and resources.
- The introduction of region/ward-wise voting enhances the system's usability and relevance for various election types, including Gram Panchayat and Nagar Sevak Elections.

The "Face Detection and Recognition Using Open CV" by Maliha Khan [3], the paper discusses the application of Intel's Open CV, a free and open-access image and videotape processing library, in the realm of computer vision. Open CV is primarily focused on tasks such as point and object recognition and machine literacy. The paper outlines the main features, OpenCV modules, and its integration with Python. It emphasizes common Open CV classifiers and operations, particularly in face recognition and image processing. Furthermore, the paper delves into erudite reviews of Open CV operations, particularly in computer vision fields such as facial expression recognition, gender identification, and face detection.

Key Features:

- The system relies on Aadhar cards, linking biometric data like fingerprints, ensuring voter authenticity.
- Utilizes biometric verification for in-person voting, reducing tampering risks and ensuring secure votes.
- Introduces a mobile app for migrants, employing Aadhar authentication and OTP for secure voting.
- Aims for 100% tamper-free votes through stringent Aadhar-based authentication measures.
- Targets the inclusion of migrants to increase the overall voting percentage in the country.
- Positioned as a cost-effective and scalable alternative to traditional Electronic Voting Machines (EVMs).
- Aligns with the Digital India initiative, integrating secure technology into the voting process for a digitally empowered society.

The “Online Voting System” by M. Rajesh [4], the paper discusses the development of a secure and user-friendly Online Voting System designed to address safety and security challenges in the voting process.

Key Features:

- The system incorporates fingerprint scanning for voter authentication, enhancing security and reducing the risk of dummy votes.
- Aadhaar card numbers are used for user login, and the fingerprint data is matched with images retrieved from the Aadhaar card database for additional verification.
- Utilizing web technologies, the system allows voters to cast their votes securely from anywhere in the country, eliminating the need to visit physical voting booths.
- The online system aims to increase voter participation by providing a convenient and fear-free method for casting votes, contributing to a higher percentage of voter turnout.
- The system improves upon existing manual and electronic voting methods, offering advantages such as accuracy, convenience, flexibility, privacy, verifiability, and mobility.
- The Election Commission of India maintains a database with complete voter information, ensuring secure storage of data and efficient management of voter details.
- The proposed system reduces costs associated with traditional methods, such as paper-based voting, and saves time by automating processes like voter registration and vote counting.
- The system introduces improvements like region/ward-wise voting, restricting voters to candidates from their specific region/ward, enhancing the system's usability and relevance for diverse election types, including Gram Panchayat and Nagar Sevak Elections.

The "Smart Online Voting System" by Neha Roy [5], this paper outlines a comprehensive system for secure online voting, leveraging face recognition, a facial camera, and OTP generation to enhance fraud prevention in both physical and earlier online voting systems. With a focus on providing a position-free voting system, particularly beneficial for individuals unable to physically attend voting locations, the system incorporates multiple layers of verification. Aadhar-based authentication, utilizing biometric data and stringent verification measures, ensures the authenticity of voters. The introduction of a mobile app for migrants facilitates secure voting, combining Aadhar authentication and OTP for enhanced security. The ultimate goal is to achieve tamper-free votes, with 100% reliability, and increase overall voting percentages. The proposed system is positioned as a cost-effective and scalable alternative to traditional Electronic Voting Machines (EVMs), aligning with the broader Digital India Initiative.

Key Features:

- The system relies on Aadhar cards, linking biometric data such as fingerprints to ensure the authenticity of voters.
- Utilizes biometric verification for in-person voting, reducing the risk of tampering and ensuring secure and authenticated votes.
- Introduces a mobile app for migrants to cast their votes, using Aadhar authentication and OTP for security.
- Aims to achieve 100% tamper-free votes by implementing stringent Aadhar-based authentication measures.
- Targets the inclusion of migrants to boost the overall voting percentage in the country.
- Compared to traditional Electronic Voting Machines (EVMs), the proposed system is deemed more cost-effective and scalable.

- Aligns with the broader national objective of promoting a digital India by integrating secure technology into the voting process.

Adida, B., Helios (2008), "Web-based open-audit voting", in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008. This paper proposes associated justify an adequate security model and criteria to judge comprehensibility. It additionally describe a web ballot theme, Pretty graspable Democracy, show that it satisfies the adequate security model which it's a lot of graspable than Pretty smart Democracy, presently the sole theme that additionally satisfies the planned security model.

Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008), "Scantegrity: End-to-end voter-veriable optical- scan voting.", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008. This paper describes Scantegrity that minimally impacts election procedures and is the first independent E2E verification mechanism that preserves optical scan as the underlying voting system and doesn't interfere with a manual recount.

Dalia, K., Ben, R, Peter Y. A, and Feng, H. (2012), "A fair and robust voting system by broadcast", 5th International Conference on E-voting, 2012. This paper proposes a recovery round to enable the election result to be announced if voters abort and also added a commitment round to ensure fairness. In addition, it also provided a computational security proof of ballot secrecy.

Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). "Star-vote: A secure, transparent, auditable, and reliable voting system", in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

This describes the STAR-Vote design, that may preferably be the next-generation electoral system for Travis County and maybe elsewhere. Recent major technical challenges relating to e-voting systems embrace, however not restricted to secure digital identity management. Any potential citizen ought to are registered to the electoral system before the elections. Their data ought to be in a very digitally processable format. Besides, their identity data ought to be unbroken personal in any involving information. ancient E-voting system could face following problems:

- Anonymous vote-casting.
- Individualized ballot processes.
- Ballot casting verifiability by (and only by) the voter.
- High initial setup costs.
- Increasing security problems.
- Lack of transparency and trust.
- Voting delays or inefficiencies related to remote/absentee voting.

2.2 Limitations of Existing Work:

While the "Secured Voting System Using Aadhar" proposed by B. Madhuri [1] offers a comprehensive solution to enhance the voting system in India, it also has some limitations:

- The extensive use of Aadhar-based authentication, particularly incorporating biometric data like fingerprints, raises privacy concerns. Critics argue that such a system may expose individuals to potential misuse or unauthorized access to sensitive personal information.
- Depending heavily on technology, especially mobile apps for migrants, introduces challenges related to connectivity, smart phone accessibility, and potential technical glitches. This could hinder the effectiveness of the proposed system, particularly in remote or underprivileged areas.

- Relying solely on Aadhar authentication might exclude individuals who, for various reasons, do not possess Aadhar cards. This could potentially disenfranchise a portion of the population, contradicting the principle of inclusivity in the electoral process.
- While the proposed system emphasizes security measures like OTP for app-based voting, any vulnerabilities in the authentication process or data transmission could pose security risks. Ensuring foolproof security in a digital voting environment is an ongoing challenge.
- Introducing a new voting system that replaces the traditional voter ID with Aadhar authentication may face resistance from various stakeholders, including citizens, political parties, and election commissions. Overcoming resistance and gaining widespread acceptance is crucial for successful implementation.
- The proposal might face legal and regulatory challenges, considering the dynamic nature of data protection and privacy laws. Compliance with existing and evolving regulations is vital to avoid legal hurdles.
- The system's reliance on mobile apps and digital platforms may exacerbate the existing digital divide, limiting the accessibility of the voting process for those who are not tech-savvy or lack access to digital devices and internet connectivity.
- Implementing a novel voting system requires comprehensive voter education programs to familiarize citizens with the new processes. Inadequate awareness and understanding could lead to confusion and potential disenfranchisement.

The "Centralized Electronic Voting System" by Prachi Zalte [2] emphasizes the imperative need for an advanced voting system in India, propelled by an increased awareness of voting and the limitations of conventional methods. The proposed system strives to elevate security, efficiency, and accessibility in the voting process by integrating biometric authentication and Aadhaar card functionality. The transition to a web-based platform is a key

feature, enabling voters to securely cast their ballots from any location, addressing logistical challenges and potentially boosting overall voter turnout. Despite these advancements, certain limitations need consideration.

- The reliance on biometric authentication and Aadhaar integration raises privacy and security concerns, with potential risks of data breaches or unauthorized access.
- The success of the system heavily depends on technology, potentially excluding voters who are not familiar with or do not have access to digital devices and the internet.
- Introducing a centralized electronic voting system may face resistance from various stakeholders, including citizens, political parties, and election commissions, affecting the system's acceptance.
- Adhering to evolving data protection and privacy laws poses challenges, requiring continuous compliance to avoid legal issues.
- The digital nature of the system may exacerbate existing disparities, limiting access for those in remote areas or with limited digital literacy.
- Implementing a novel voting system necessitates extensive voter education to ensure citizens understand and trust the new processes, which might be challenging.
- The transition to a centralized electronic system incurs initial implementation costs, potentially straining resources and budgets.

The "Face Detection and Recognition Using Open CV" by Maliha Khan [3] explores the application of Intel's Open CV in computer vision, focusing on tasks like face recognition and image processing. The paper details Open CV's modules, features, and integration with Python, emphasizing its role in facial expression recognition, gender identification, and face detection. Key features include reliance on Aadhar cards for voter authenticity, biometric verification for in-person voting, and a mobile app for secure voting by migrants. However, certain limitations need consideration:

- The reliance on Aadhar cards and biometric data raises privacy concerns, necessitating robust measures to safeguard sensitive information and prevent unauthorized access.
- The success of the system heavily relies on technology, potentially excluding individuals with limited digital literacy or access to advanced technologies.
- The use of facial recognition technology prompts ethical considerations related to consent, data usage, and potential biases in the recognition algorithms.
- Facial recognition systems may face challenges in accuracy, particularly in diverse demographic settings, potentially leading to misidentifications or biased outcomes.
- Introducing advanced technology like facial recognition may face resistance from individuals skeptical about its reliability, potentially affecting its widespread acceptance.
- Adhering to evolving data protection and privacy laws poses challenges, requiring continuous compliance to avoid legal issues.

The "Online Voting System" by M. Rajesh [4] aims to address safety and security challenges in the voting process through a secure and user-friendly online platform. While the key features highlight its strengths, it's essential to consider certain limitations:

- Despite fingerprint scanning and Aadhaar authentication, online systems are susceptible to cyber security threats, including hacking and unauthorized access, potentially compromising the integrity of the voting process.
- Relying on web technologies may exclude individuals with limited access to the internet or digital devices, potentially leading to unequal participation and representation.
- The use of Aadhaar data and fingerprint information raises privacy concerns, necessitating stringent measures to ensure the confidentiality and ethical handling of sensitive voter data.

- Introducing online voting may face resistance from individuals accustomed to traditional voting methods, and addressing this resistance is crucial for widespread acceptance and participation.
- The system's effectiveness heavily relies on the reliability of web technologies and digital infrastructure, requiring continuous maintenance and updates to prevent technical glitches or failures.
- Adhering to evolving data protection laws and ensuring legal compliance is imperative to avoid legal challenges related to voter data security and privacy.
- Successful implementation relies on voters' understanding and trust in the online system, necessitating comprehensive education campaigns to familiarize voters with the new platform and its security measures.

The "Smart Online Voting System" by Neha Roy [5] aims to enhance fraud prevention in both physical and online voting systems through the integration of face recognition, facial cameras, and OTP generation. While highlighting its key features, it's essential to consider potential limitations:

- The use of face recognition and Aadhar authentication raises privacy issues, necessitating robust measures to safeguard the confidentiality and ethical handling of sensitive biometric data.
- The effectiveness of the system heavily relies on the reliability of face recognition technology, facial cameras, and OTP generation. Technical glitches or failures may impact the overall integrity of the voting process.
- Dependency on a mobile app for migrants may exclude individuals with limited access to smart phones or digital devices, potentially leading to disparities in voter participation.

- Introducing advanced technological features may face resistance from voters unfamiliar with or skeptical about such systems, requiring comprehensive education and awareness programs.
- The online nature of the system makes it susceptible to cyber security threats, including hacking and unauthorized access, necessitating robust cyber security measures to prevent tampering.
- Adherence to data protection laws and ensuring legal compliance is crucial to avoid legal challenges related to voter data security, privacy, and the use of biometric information.

In this study S. J. J. Arputhamoni et al. (2021) [1], have put forth a proposition for an online voting system that incorporates the utilization of biometric authentication, specifically in the form of facial and fingerprint recognition. Additionally, image processing techniques and a convolutional neural network (CNN-S) have been employed. The objective of this system is to augment the security and precision of online voting by ensuring the authentication of voters. Biometrics assume a pivotal role in the verification of voters, while image processing techniques are implemented to enhance the quality of biometric data. The CNN-S is utilized for the purpose of extracting features, thereby enhancing the overall dependability of the authentication process. The focus of the paper is to overcome the traditional limitations associated with voting and to heighten the security and accessibility of online voting.

In this research G. Prabhu et al. (2021) [2], proposed the development of a secure internet voting system that addresses the limitations of India's current offline voting system. This proposed system integrates face recognition technology and OTP authentication to enable remote voting through computers or mobile phones, thereby enhancing accessibility and efficiency. Furthermore, it provides the opportunity for offline voting using RFID tags.

The main objective of proposed system is to streamline the voting process, ensure transparency, and reduce the requirement for extensive manual labor. RFID tags, issued by the government, are utilized by offline voters and are verified by RFID card readers. Online voters are required to register their facial features in the system, with multiple instances captured to ensure accuracy. The voting process includes a two-step authentication process: facial recognition and OTP verification, which uphold the security of the vote. The results can be accessed in real-time through a central database, thereby further enhancing transparency and efficiency.

According to A. S. Andekar et al. (2022) [3], presents a novel E-voting framework predicated on facial recognition. The framework is devised with the intention of ensuring security, convenience, and the absence of malpractice. It employs a three-tier security model, encompassing the verification of Aadhar ID and Unique voter ID by means of mobile number OTP verification, facial recognition, and captcha verification. Additionally, the framework utilizes the Local Binary Pattern Histogram (LBPH) for facial recognition, which attains an accuracy rate of 89%. The article also delves into the potential predicaments that may arise in the operation of the system, such as twin identification, variations in acquisition and physical appearances, as well as the challenge of storing vast and sensitive data. The article suggests resolutions to these challenges, such as verifying the UID number and Aadhar number by cross-referencing with the pre-registered voter database. It also recommends ensuring a reliable internet connection, capturing real-time facial impressions and current physiological features during registration, organizing data through a suitable format and structure, storing it securely on the cloud, and allowing administrators to access location-specific data stored in the cloud.

In this research Nilam Choudhary et al. (2021) [9], proposes a novel voting system that offers heightened security through the implementation of three levels of verification. The

initial level entails the creation of a distinctive identification number for voters at the time of registration. The subsequent level involves the diligent cross-verification of these identification numbers by the Election Commission Officers. Lastly, the third and most pivotal level incorporates the utilization of facial recognition technology, wherein the current facial attributes of voters are compared with those stored in a comprehensive database, thereby mitigating the occurrence of fraudulent voting. The research delves into an exploration of diverse facial recognition algorithms, namely Eigen faces, Fisher faces, and SURF (Speeded Up Robust Features), and provides an in depth comparative analysis of their respective performance. Eigen faces rely on Eigenvectors for facial identification and are founded on the principles of Principal Component Analysis (PCA). Conversely, Fisher faces expand upon the concept of Eigen faces by integrating both PCA and Linear Discriminant Analysis (LDA) to yield superior outcomes, particularly in scenarios involving fluctuations in lighting conditions and facial expressions. In contrast, SURF represents an algorithm that facilitates scale and rotation-invariant feature detection, rendering it highly resilient for both object and facial recognition.

In this research, N. Roy, et al. (2023)[4] suggests an original approach to enhance the security and verifiability of online voting. This approach incorporates the utilization of one-time password (OTP) authentication and facial recognition. The proposed system implements a two-step verification process, where voters initially authenticate their identity by using their Aadhaar card, and subsequently validate themselves through their face and an OTP delivered to their mobile phone. Additionally, this system makes use of a database containing the information of registered voters, guaranteeing that only eligible individuals are allowed to exercise their voting rights.

Current significant technological issues with electronic voting include, but are not limited to, safe digital identity management. Before the elections, every prospective citizen

should register with the electoral system. Their information should be processed digitally for the mat. Additionally, their identifying information should be completely private in any involved information.

Ancient E-Voting System Might Face Following Problems:

Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system.

- Individualized ballot processes: How a vote are depicted within the involving net applications or databases continues to be AN open discussion. Whereas a transparent text message is that the worst plan, a hashed token is wont to offer obscurity and integrity. Meanwhile, the vote ought to be non-reputable, that can't be bonded by the token resolution.
- Ballot casting verifiability by (and only by) the voter: The elector ought to be ready to see and verify his/her own vote, when he/she submitted the vote. This is often vital to realize so as to forestall, or a minimum of to note, any potential malicious activity. This counter live, except for providing suggests that of non-repudiation, can sure boost the sensation of trust of the voters. These issues area unit partly self-addressed in some recent applications. Yet, suggests that of e-voting is presently in use in many countries together with Brazil, UK, Japan, and Republic of Estonia. Republic of Estonia ought to be evaluated otherwise than the others, since they supply a full e-voting resolution that's, said to be, equivalent of ancient paper-based elections.
- High initial setup costs: Though sustaining and maintaining on-line selection systems is way cheaper than ancient elections, initial deployments could be pricy, particularly for businesses.
- Increasing security problems: Cyber attacks cause an excellent threat to the general public polls. nobody would settle for the responsibility if associate degree hacking try

succeeds throughout an election. The DDoS attacks are documented and largely not the case within the elections. The citizen integrity commission of the us gave an affidavit concerning the state of the elections within the North American country recently. Accordingly; Ronald Rivest explicit that "hackers have myriad ways in which of assaultive pick machines". As associate degree example; barcodes on ballots and smart phones in pick locations may be utilized in the hacking method. Apple explicit that we tend to mustn't ignore the actual fact that computers are hackable, and also the evidence will simply be deleted. Double-voting or voters from the opposite regions also are some common issues.[8] To mitigate these threats, software mechanisms which promise the following should be deployed:

  - Prevention of evidence deletion.
  - Transparency with privacy.

- Lack of transparency and trust: How can people surely trust the results, when everything is done online? Perceptual problems cannot be ignored.
- Voting delays or inefficiencies related to remote voting: Timing is very important in voting schemes; technical capabilities and the infrastructures should be reliable and run at the highest possible performance to let remote voting be synchronous.[5]

In [3], the author specified mainly on securing the voting system, by comparing the insecurities that exist in the manual voting system to that of the electronic voting system. Authors in [4] suggested the use of Remote Internet Voting, with a view to enhance voter convenience, increase voter confidence and voter turnout. In the survey, authors suggested remote poll-site electronic voting as the best step forward as it provides better voter convenience, but at the same time, does not compromise security. In [5], the author review the security measures needed for remote online voting system by focusing on two cases where voters cast their ballots over the Internet – the 2000 Arizona Democratic Primary and the

University of Virginia Student Council Elections. The author claims that a secure voting system must thoroughly satisfy four major requirements: authentication, availability, confidentiality and integrity.

In [6], the author reviewed e-voting procedure by describing its advantages and disadvantages. His work majored were on the security measures such as firewalls or SSL communications which are necessary but not sufficient to guarantee the specific security requirements of e-voting. Also, the author describes the additional layer of specialized security technology to address the specific risks posed by electronic voting and guarantee critical security requirements such as voters' privacy, vote integrity and voter-verifiability. The author equally suggested the use of Biometrics and smartcard for authenticating users. One major issue the author stressed out is the difference between biometric authentications compared to "classic" authentication like smart cards.

The e-voting system proposed in [6] does not interact in any way with the biometric characteristics of the actual users, but still authenticates the user with the help of the user's authentication certificate on the smart card.

In [7], authors lay emphasis on the rapid advancement in Information and communications technologies which has given rise to new applications that were impossible just few years ago. This paper details the requirements, design and implementation of a generic and secure electronic voting system where voters can cast their votes anytime, anywhere and using a number of electronic devices including private computer networks, web and mobile phones. Authors in [7] also compared both the manual voting system with electronic voting system and evaluate the flaws of manual voting system in relation to how the electronic voting system can improve the flaws. Further work was reviewed by the author in a bid to make and electronic voting system work on various platforms.

In [8], the author specified on the authentication methodology in securing transaction, through the use of multilayered encryption algorithms. The author laid emphasis on the use of multifactor authentication method, which includes both the mobile station authentication and the financial institution authentication.

In [1], the author describes the security features of the electronic voting system and e-voting system is better than manual voting system. Also, the author shows that voters, without any insider privileges, voter can cast unlimited votes without being detected by any mechanisms within the voting terminal software.

Also in [13], authors presented the design and development of real time of an electronic-voting system with emphasis on security and result veracity for increase in the efficiency in electoral process and compensate for challenges in manual voting in a multi-ethnic and diverse climate like Nigeria. In this paper we present the design and development of a multifaceted cryptographic model for a secured electronic voting system in e-democratic engendered countries where emphasis is placed on conducting transparent, fair and trusted elections.

CHAPTER III

A SURVEY ON THE ELECTRONIC VOTING SYSTEMS

Electronic voting is a topic of active debate; many people, although acknowledging that paper-based voting systems are outdated and require cumbersome labor, have a hard time trusting electronic voting and the security risks it brings. However, in the era of the Internet and Web and mobile applications that boomed and became important, and now in our days, because of the recent pandemic and sanitary restrictions. COVID-19 further highlighted the need to improve the current voting system, which already changed many sectors, voting in person, and going to a polling station crowded with people is against the pandemic guidelines. In countries where the option of online voting is not provided, voters will have to choose between putting themselves in danger of exposure to the virus or staying home and not voting.

Existing voting systems are divided into two main types: traditional methods and electronic voting methods. In traditional methods, voters mark paper ballots by hand [4] or involve mechanical lever machines [5]. Within electronic voting [6], there are many types such as punched-card [7], direct recording electronic [8], optical scanning systems [9], vote recorder [10], i-voting [11], and so forth [12]. Table categorizes some existing voting systems.

The continued reliance on traditional voting systems, corruption becomes far too easy, resulting in the voice of the people not being clearly heard or completely drowned out in fraud. In 1981, Chaum [13] was the first to use cryptography to secure elections, as suggested in his famous paper on anonymous communications. He described new primitives in cryptography that can be used as building blocks in different applications, including remote electronic elections. Therefore, the time he first proposed the end-to-end verifiable voting

(E2E) scheme was his votegrity scheme. Other E2E schemes later emerged from Chaum's solution, such as:

- Neffs Markpledge [14]. Markpledge was the first E2E voting protocol that was offered alongside voice, including the development of the other E2E schemes.
- Ryans Pêt à Voter [15] provides an accurate election from end-to-end with an easy and familiar voter experience. It warrants a great degree of transparency while preserving the privacy of the ballot.
- Helios [16], a university voting system, underwent a security scan, which revealed security vulnerabilities that could affect the election outcome. This guided the development of new versions (Helios 2.0 and Helios 3.0) to fix the vulnerabilities reported in [17].
- Star-Vote (A Secure, Transparent, Auditable, and Reliable Voting System) [18] implements the homomorphic tally technique [19]. Homomorphic tally implicates changes, generally additions and multiplications, to the cipher text, which are preserved during decryption to reveal operations that were effected on the cipher text when retrieving the changed decrypted value.
- Zeus [20] and Apollo [21] are using Helios to construct their voting protocol while trying to address certain security problems inherent in the Helios voting system. For example, Apollo solves cross-site scripting (XSS), cross-site tampering, clash attacks, and click jacking with the support of voting assistants. The XSS is in the third position of the top web frameworks, as found by the Open Web Application Security Project in 2013 [22].
- Follow My Vote [23] is a framework that has a secure online blockchain voting system with the ability to audit the ballot box to see the real-time democratic development.

- TIVI (accessible and verifiable online voting) [24] is a remote voting platform that is considered the most advanced, secure, and universally accurate online voting solution for governments. It guarantees the end-to-end integrity of the distant voting process. TIVI was designed and developed by globally known experts in election technology, cyber security, information security, identity management, and verifiable cryptography.
- Ethereum [25] is a decentralized exchange protocol that establishes a peer-to-peer network and allows users to create smart contracts. These contracts are based on an application code to verify or enforce a mutual contract.
- Zcash [26] is a decentralized blockchain payment system that aims to ensure the anonymity of transactions. To expedite the transactions, Zcash implements zk-SNARKS (zero-knowledge succinct non interactive arguments of knowledge) designed in the lib-snark library.
- Hyperledger [27] is an open-source distributed ledger framework and enterprise-grade codebase that aims to identify and realize a cross-industry open standard platform for distributed ledgers that can transform the way business transactions [28].

Analyzing these schemes shows how hard it is to maintain both security and transparency while achieving E2E verifiability. This leads us to think of blockchains that can help to meet this requirement. However, we believe that the blockchain represents a new solution that by its nature many security concerns [29]. There have also been numerous research about the utilization of blockchain to create decentralized electronic online voting. With blockchain gaining momentum as the decentralized trust protocol, we can imagine its utilization of it as a backbone of an electronic voting system. Blockchain will ensure a trust protocol in which voters do not have to implicitly trust the credibility of the voting system and its administration. Blockchain will ensure transparency and E2E verifiability.

The electronic voting system was and remains a hot topic in research. In this section, we give a summary of these works related to the electronic voting system. In the early 1980s, Chaum [13] introduced an electronic voting system based on the Theorem of Blind Signature; the purpose was to hide voter identity by using public-key cryptography and corrupting the link between the voter and their ballot. Many papers were published in this regard [30-32], they all used some type of cryptographic techniques to achieve secrecy in an e-voting scheme. Elgamal [30] proposed the implementation of the Diffie-Hellman key distribution scheme, in a public key cryptosystem. Articles [31] and [32] use blind signatures and digital signatures, respectively, for confidentiality and the voter's digital signature during authentication.

The first country to have a national electronic election system was Estonia in 2007 [33], the system was called i-voting and it allows citizens to cast their vote remotely via the internet, all thanks to an ID card, an electronic national identification card that enables authentication and electronic encrypted signature using both Secure Hashing Algorithms SHA1 and SHA2. The Estonian ID card also allows access to different Estonian E-services like health insurance, bank accounts, and proof of identity within the EU. The Estonia electronic system, although successful is still a black box, and it is hard to tell if they respect voter anonymity because it is not auditable by voters and it requires putting trust in the government. Norway also launched an electronic voting system project for the country council elections back in 2011, but unfortunately, the project was ceased because of some security concerns [34]. Both systems' transparency is in question, so an auditable open-source system is needed for a trusted election. Another problem is that both systems are centralized, which puts them in danger of distributed denial-of-service attacks.

Research articles have also been done on applying homomorphic encryption and the ZKP in [35-37]. In Iversen's [35] study, the author(s) proposed using interactive ZKP (IZKP) techniques to initialize voters. In Schoenmakers's [36] study, the author described a publicly

verifiable secret sharing scheme with optimal running time, which can be used for an election application scheme. The purpose of ZKP is to verify the validity of the ballot without revealing the choice made by the voter. The authors in Cramer et al.'s [37] study used the factoring assumptions in their voting scheme.

Other proposals were based on blockchain technology [38, 39]. Both [38] and [39] leveraged blockchain technology to create an e-voting system. The con of these proposed systems is the lack of voter privacy by binding the voter ballot with their respective identity on the blockchain. On the blockchain, every node is represented by its public address, other voters might not know the person behind that address but the committee that allowed eligible people to participate knows their corresponding address, therefore voters are not fully anonymous.

CHAPTER IV

FACIAL RECOGNITION ENABLED ONLINE VOTING SYSTEM

4.1 Authentication Module:

The Authentication Module for this project incorporates robust security measures, particularly evident in the Admin Login functionality. Leveraging Django's built-in authentication system, this module establishes a secure gateway for authorized administrators to access the backend.

By utilizing industry-standard authentication protocols, the system ensures that only personnel with valid credentials can log in, safeguarding sensitive election-related data and administrative functionalities. This approach not only fortifies the system against unauthorized access but also aligns with best practices for securing the online voting platform, laying a foundation for trustworthiness and integrity in the electoral process.

4.2 Citizen Management Module:

In the Citizen Management Module, the registration process involves citizens uploading a photo rather than capturing it in real-time. During Citizen Registration, eligible voters are required to provide a pre-existing photo of themselves, which is then securely stored in the system. This approach allows for a more flexible and user-friendly registration experience, as citizens can select a suitable photo at their convenience.

The system then processes and stores the uploaded photo, associating it with the citizen's biometric profile for subsequent facial recognition verification during the login process. This distinction between uploading a photo during registration and utilizing facial recognition during login ensures a seamless and accessible user experience while maintaining the security and integrity of the online voting platform.

4.3 Election Management Module:

Within the administrative functionalities of this project, the Add Elections and Add Candidates modules play pivotal roles in orchestrating the electoral landscape. The Add Elections feature empowers administrators to effortlessly set up new elections, offering a comprehensive interface to define essential details such as the type of election and the list of candidates. This module acts as the gateway for administrators to establish the groundwork for a transparent and efficient voting process.

Complementing this, the Add Candidates module provides administrators with the flexibility to manage candidate details dynamically. It facilitates the addition or removal of candidates associated with each election, ensuring an adaptable and responsive system that accurately represents the choices available to the voting populace.

Together, these modules contribute to the seamless administration and organization of elections within the online voting platform, reflecting the project's commitment to user-friendly and robust electoral management.

4.4 Voting Module:

Real-time Facial Recognition: Integrates Haar-like features and the K-nearest neighbors (KNN) algorithm for real-time facial recognition during the voting process, ensuring secure and accurate voter authentication.

The Haar Cascade algorithm is a machine learning object detection method used to identify objects in images or video. It's particularly popular for face detection but can be trained to recognize other objects as well. The algorithm works by training on positive and negative images.

The K-Nearest Neighbors (KNN) algorithm is a simple and effective classification algorithm based on the concept of proximity. Here is a concise explanation of the KNN algorithm:

- Training: Store all the training examples.
- Input (Test Instance): Receive a new instance to be classified.
- Calculate Distances: Calculate the distance between the test instance and all training instances. The commonly used distance metric is Euclidean distance, but other metrics can be used based on the application.
- Sort Distances: Sort the distances in ascending order.
- Choose K Neighbors: Select the top K training instances with the smallest distances to the test instance.
- Majority Voting: Count the occurrences of each class label among the selected K neighbors.
- Assign Class Label: Assign the class label that has the highest count as the predicted class for the test instance.

The Vote Casting module is a pivotal component of this project, providing registered citizens with a secure and streamlined mechanism to exercise their voting rights. Through a user-friendly interface, citizens can confidently cast their votes for their chosen candidates or ballot options. The module ensures the integrity of the voting process by incorporating security measures such as facial recognition, which authenticates the user before allowing the vote to be securely cast and counted. This seamless and accessible voting experience enhances civic participation, contributing to a reliable and trustworthy online voting system.

4.5 Announcement Module:

The Announcements module within the administrative functionalities of this project serves as a vital communication channel between administrators and citizens. This feature empowers administrators to disseminate crucial election-related information, fostering transparency and keeping citizens informed.

Through a user-friendly interface, administrators can make announcements, ensuring that citizens are well-aware of essential updates, deadlines, or any pertinent details related to the ongoing electoral process. By facilitating effective communication, the Announcements module contributes to an informed and engaged electorate, promoting trust and participation in the online voting system.

4.6 Feedback Module:

The Feedback Submission module plays a crucial role in fostering citizen engagement and contributing to the refinement of the online voting system. This feature allows registered citizens to share their valuable feedback on various aspects of the voting process, system functionality, or any relevant concerns they may have encountered. By providing citizens with a platform to voice their opinions, the module promotes transparency and responsiveness within the electoral framework.

The collected feedback becomes instrumental in implementing continuous improvements, ensuring that the online voting system evolves to meet the needs and expectations of its users. This user-centric approach enhances the overall effectiveness and reliability of the voting experience.

4.7 User Interface Module:

The implementation of HTML and CSS design in the project contributes to the creation of visually appealing and user-friendly interfaces across different modules. HTML, the standard mark-up language, structures the content of web pages, while CSS enhances the presentation, ensuring a cohesive and aesthetically pleasing look. This combination results in interfaces that are intuitive, responsive, and accessible, catering to both administrators and citizens.

The use of HTML and CSS underscores the commitment to a positive user experience, facilitating seamless navigation and interaction within the online voting system.

4.8 Security Module:

The sha256() function in Python, part of the hashlib library, is a constructor for creating SHA-256 hash objects. Internally, it utilizes the SHA-256 cryptographic hash algorithm, which is a member of the SHA-2 family. The SHA-256 algorithm performs a series of well-defined steps to produce a fixed-size (256-bit or 64-character hexadecimal) hash value. Here's a simplified overview of what happens internally:

- Arbitrary length message string 'M'
- Convert it to binary.
- Pre-processing Stage:
- Padding a message M
- Parsing the Message M
- Setting initial hash values Ho..... H
- Hash Computation
- Prepare the Message Schedule
- Initialize a, b, c, d, e, f, g and h
- Compute for the intermediate hash values
- Append Hash values Ho, H1, H2, H3 H4 H5 H6H,
- 256-bits Message digest.

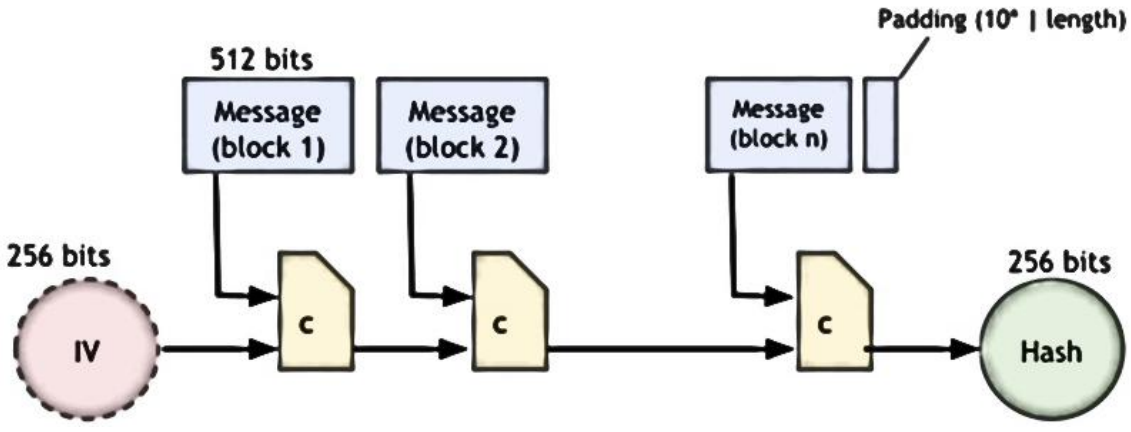


Figure 2.1: SHA-256

4.9 Reporting and Analytics Module:

The Election Results module plays a pivotal role in the project by dynamically generating and presenting real-time election outcomes. This feature ensures that both administrators and citizens have immediate access to the latest information, fostering transparency and credibility in the electoral process.

By offering up-to-date results, the module empowers administrators to make informed decisions, while citizens gain timely insights into the progress of the elections. The real-time nature of the Election Results module enhances the overall user experience, contributing to the integrity and openness of the online voting system.

CHAPTER V

BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEM INCORPORATING CRYPTOGRAPHIC METHODS

The simple rationalization could be a 'chain' of blocks. A block is associate degree mass set of information. Knowledge square measure collected and method to suit in an exceedingly block through a process known as mining. Every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block. During this method, all the information may be connected via a connected list structure.

5.1 Analysis / Framework / Algorithm:

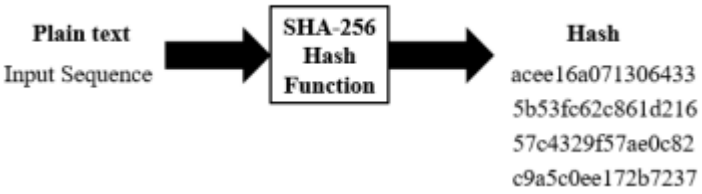


Figure 5.1: SHA-256 Algorithm Working

Working:

- The SHA-256 algorithm takes an input of any random length and produces an output of a fixed length (256 bits).
- In the case of SHA-256 algorithm no matter how big or small is the input, the output is of fixed length (256 bits).

A Cryptographic Hash Function has the Following Properties:

- Deterministic: This means that no matter how many times we enter the same input we will get the same result.

- Quick Computation: This means that the result is generated quickly, and this leads to an increase in the system efficiency.
- Pre-Image resistance: Suppose we are rolling a dot (1-6) and instead of getting a specific number we get the hash value. Now we calculate the hash value of each number and then compare it with the result. And for larger data sets it is possible to break pre-Image resistance by brute force method and this takes too long that it does not matter.
- Small changes in Input change the whole Output: A minor change in the input significantly changes the whole output.
- Collision Resistant: Every input will have a unique hash value.
- Puzzle friendly: The combination of two values gives the hash value of new variable.

The Need of Hashing in Blockchain:

- The blockchain is a sequence of blocks that contain data.
- Each block has a hash pointer that contains previous block's data.
- So if a hacker tries to attack a particular block, the changes will be reflected to the entire chain of blocks.
- Therefore, the blockchain concept is so revolutionary.

5.2 Transactions within the Ethereum:

Blockchain in an Ethereum smart contract, agreements between contributors are written right into program code on an if-when statement. When the requirements of the if-when statements are met, the program code executes the terms of the smart contract. Contract execution begins with a transaction in which one of the contributors instructs the smart contract to do a certain task.

The Ethereum node receives this transaction and then moves it onto the smart contract, indoor a virtual machine (VM). This VM is simulated in the smart contract takes the

transaction as an input on a blockchain and runs it like software in which all contributors in the smart contract can watch the updates. The codes in the smart contract are distributed between all contributors, as there is no centralized authority that holds all the statement documents and controls the process. The blockchain allows various participants to agree to or do modifications to the smart contract, via their access passes. The transactions within the Ethereum blockchain network.

A Transaction has the Following Parameters:

- From: The sender's 20-byte address (user in Ethereum network), it is the account that initiates the transaction.
- To: The 20-byte recipient address, it is the account that receives the transaction, and it can be an externally owned account (EOA), a smart contract account, or none.
- Value: The total amount of Wei fund (1 ether=1018 Weis) to transfer to an EOA or smart contract account. Wei represents the smallest unit (denomination) of ether-the crypto currency coin used on the Ethereum network from which a user may make a transaction.

5.3 Blockchain-Based Voting System:

A typical architecture of the blockchain-based voting system is presented in Figure 5.2. Voters send their personal data to administrators for verification via their devices, which we assume to be secure. The interaction between voters and system administrators is off chain, which means that it is not part of the blockchain system. When a voter's identity is confirmed, the administrators issue the tokens that let voters to cast their vote into the blockchain.

Eligible voters receive one token in their blockchain application that acts as an electronic wallet; it is also the interface to interact with the blockchain to vote and audit. The token can only be used once and cannot be transferred or sold between wallets. When a voter

wants to fill out his ballot to cast the vote, the application generates a zero-knowledge set membership proof (ZKSMP) code to prove the validity of the choice made without having to reveal it; the vote must be within a list of candidates predefined by the administrators. So, both the token and the code will be used to validate the ballot; this will eliminate the risk of Sybil attacks. All voters must cast their ballot within a period previously configured by the administrators. Proof of Authority validators act like miners in the Bitcoin blockchain system. They validate transactions and add them to the blockchain over the voting phase.

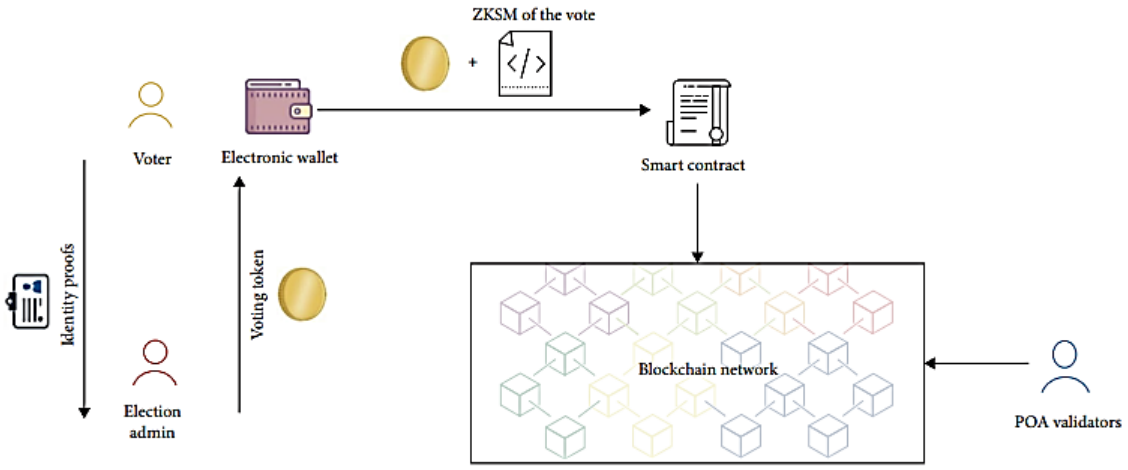


Figure 5.2: Typical scheme of blockchain-based voting system

5.4 Implementation Tools:

To implement a blockchain-based electronic voting system, the following tools can be used:

- Go-Ethereum: Go-Ethereum (aka Geth) is a tool to implement Ethereum blockchain built using Go programming language to run smart contracts and decentralized applications. Go-Ethereum has a decentralized machine based on consensus algorithms such as Proof of Work [9], Proof of Activity [10], or Proof of Stake [11].
- Ganache is an isolated personal blockchain for testing smart contracts and developing distributed applications on the Ethereum blockchain [12].

- Truffle is a development environment that includes a collection of implements for developing decentralized applications in the Ethereum blockchain [13].
- MetaMask is a browser-based wallet crypto currency software used to interact with the Ethereum network. It is used to manage transactions, keys, and user accounts in Ethereum blockchain networks [14].
- Hyperledger Avalon is a popular Hyperledger development tool [15] that addresses major issues for blockchain-based electronic voting system such as confidentiality, integrity, and scalability by incorporating ZKP, trusted execution environments [16], and multiparty compute [17]. There are other tools for Hyperledger development such as Caliper, Cello, Explorer, Cactus, and so forth [18].

CHAPTER VI

E-VOTING SYSTEM USING MULTIFACTOR AUTHENTICATION AND CRYPTOGRAPHIC HASH FUNCTIONS

Democratic governance is based on elections which allow the populace to choose their representatives and express their preferences for tenure based leadership. Naturally, the integrity of the election process is fundamental to the integrity of democracy [10]. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent such that voters and candidates can accept the results of an election [19].

In traditional voting system, the primary means of voting embraces physical balloting of voters' intent. The paper ballots are read and interpreted. The results of each candidate are individually tabulated and displayed. The physical presence of the voter is required where by the thumbprint of individual registered voter is used to vote. Although, the design of a voting system whether electronic, paper ballots or mechanical devices must satisfy a number of competing criteria [7, 20]. These criteria are the anonymity and tamper resistance of a voter's ballot, both to guarantee the voters' safety when voting against a malevolent candidate; and to guarantee that voters have no evidence that proves which candidates received their votes. The existence of such evidence would allow votes to be purchased by a candidate [21]. The voting system must also be tamper-resistant to avoid a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders [21].

The conventional system of voting is characterized with high rate of fraudulent practices ranging from stolen of ballots, falsification of vote counts or rigging, improper voting and votes lost through invalid ballot marks due to ignorance and inadequate prior awareness and negligence [22]. This voting system is insecure and has been characterized with suits of election malpractices. The most fundamental problem is that the entire election

hinges on the correctness, robustness, and security of the software within the voting terminal. With this, due to the high rate of election malpractices, secure electronic voting system is proposed based on multifactor authentication of voters and cryptographic hashed electronic vote.

The current single factor authentication technique embraced in electoral process of most developing countries is not very secure to protect users from identity theft. Single factor authentication increases risks posed by phishing, identify theft, online fraud and loss of confidence on democratic decision making process. So, voting systems need to implement an effective multifactor authentication system to reduce fraud and make elections fair, free and credible.

E-voting refers to an election or referendum that involves the use of electronic means in at least the casting of the vote [23]. Once recorded, the elector's vote is dispatched in real time to a secure electronic vote store, where it is held prior to counting. The presence of electronic voting system to voting brings a lot of security measures into the voting system, thus, eradicating issues such as stolen of ballots, falsification of vote counts or rigging, improper voting and vote lost through invalid ballot marks due to ignorance and inadequate prior awareness and negligence, allocation of vote counts and other theft activities related to the traditional voting system [29, 20, 23]. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. In an attempt to achieve security measures in e-voting system, major security features to fulfill are Confidentiality, Integrity, Non-repudiation and Authentication [24].

Voting is a vital part of the democratic process. As such, the efficiency, reliability, and security of the technologies involved are critical. In this paper, we present the design and development of a multifaceted cryptographic model for a secured electronic voting system in

e-democratic engendered countries where emphasis is placed on conducting transparent, fair and trusted elections. The designed system is practically aimed at securing electronic voting system by ensuring authentication and integrity in transmission of data flows in the network.

System Design:

The purpose of system design is to create a technical solution that satisfies the functional requirements for the system. The functional specification produced during system requirements analysis is transformed into a physical architecture through system modeling and database design.

A. Requirements Definition for the Secure E-voting System:

According to the literature, the design of any voting system must satisfy a number of competing criteria [23, 26, 27, and 22]. These requirements give an avenue for a free, fair, credible and confidential election. These requirements by [25] are grouped into generic and system specific; by [32] as functional and non-functional requirements. Considering evoting from functional and non-functional point of view, the following requirements are necessary:

- Confidentiality: Ensuring that no one can read the message except the intended receiver.
- Non-repudiation: A mechanism to prove that the sender really sent this message.
- Authentication: Only the eligible and authorized voters can vote through the system.
- Accuracy: Every voted ballot should be correctly counted into the final tally within the tolerable extent of error.
- Integrity: Votes should not be able to be modified, forged or deleted without detection
- Secrecy and Non-Coercion: Only voters know what they vote for. Voters must not be able to prove what they vote for in order to reduce the risk of coercion and vote-buying activity.

- Audit trail: The system should provide the mechanism for audit trail. Audit trail can help to verify that the votes are accounted correctly in the tally and maintain the security for the system.
- Uniqueness: Every voter has the same number of the votes. No one can vote more times than others.
- Transparency: The election process should be transparent to the voters. Voters can clearly understand the mechanism of the electronic voting system and know whether their votes have been correctly counted.
- Simplicity: The system should be designed user friendly. It should also meet the need of the disabled and illiterate.
- Democracy: Permits only eligible voters to vote only once.
- Privacy: All votes remain secret while voting takes place and each individual vote cannot be linked by any individual to the voter who casts it. The privacy issue is paramount.
- Accuracy: The voting result accurately reflects voters' choices. In this case, no vote can be altered, duplicated or eliminated without being detected.
- Fairness: No partial result is available before the final result comes out.
- Security: Votes should not be manipulated during the whole process of voting.
- Verifiability: Voting systems should be verified so as to have confidence that they meet necessary criteria.

B. Architecture of Secured Model for E-Voting System:

The electronic voting system was designed to enable the overall populace to vote over wireless medium, and the system is opened to the voter and the administrator. The primary aim of the design is to provide a secured system over wired and wireless connection. The design architecture follows conceptual perspective of the three layered Organization for the

advancement of Structured Information Standards (OASIS): the pre-election phase, election phase and the post-election phase shown in figure 6.1.

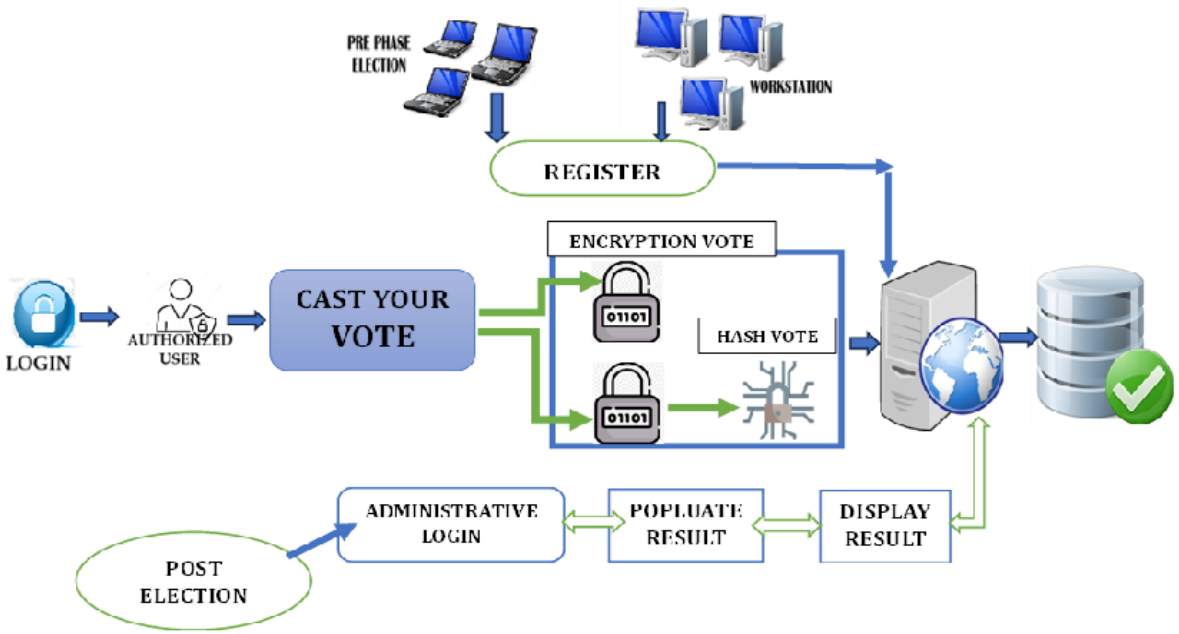


Figure 6.1: System Architecture of the Secured Voting System

The pre-election phase provides an aspiring voter a phase to register his/her identity into the system. The process involved includes providing input access for qualified voter, and thereafter, the system automatically generates a unique id, unique grid card that matched directly with the unique id generated by the system, and then a unique short message service (SMS) one time pin is also generated by the system.

This generated on time random array of pin is then automatically sent to the aspiring voter in a form of Short Message Service (SMS) to the user if he/she meets the requirement to vote. The pre-election has several operations involved in it. The first operation involves the registration phase, whereby each aspiring client registers his/her profile.

During registration, some fields such as phone number and email address would be made mandatory for clients to fill data in. After registration, a soft random grid card code is generated by the system for each user. Also, an SMS containing random array of America

Standard Code for Information Interchange (ASCII) would be sent to the registered clients' phone number.

All details pertaining to registration is stored in the database. The election phase involves voting, the voter uses the randomly generated SMS pin, and then the grid card code, to vote, coupled with his/her registered number (unique id). The vote when casted is encoded with a private key.

The encoded result is divided into two parts. One part of the encoded result is further hashed using the SHA256 (secured hash function) and a 256 bit of random number is generated. The first encoded result and the hashed function is then sent to the database to be processed at the post-election phase. Figure 6.2 and figure 6.3 shows the diagrammatic flow of these vote integrity check of the election phase.

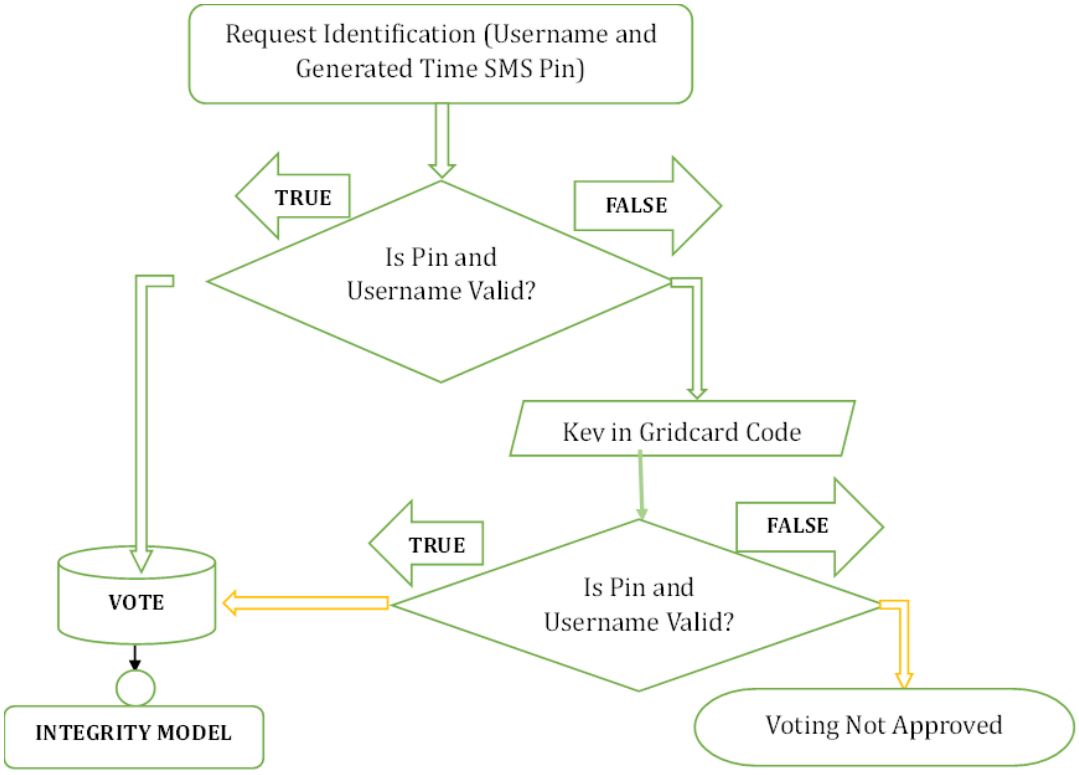


Figure 6.2: Secure E-voting Election Phase for voter's authentication Check

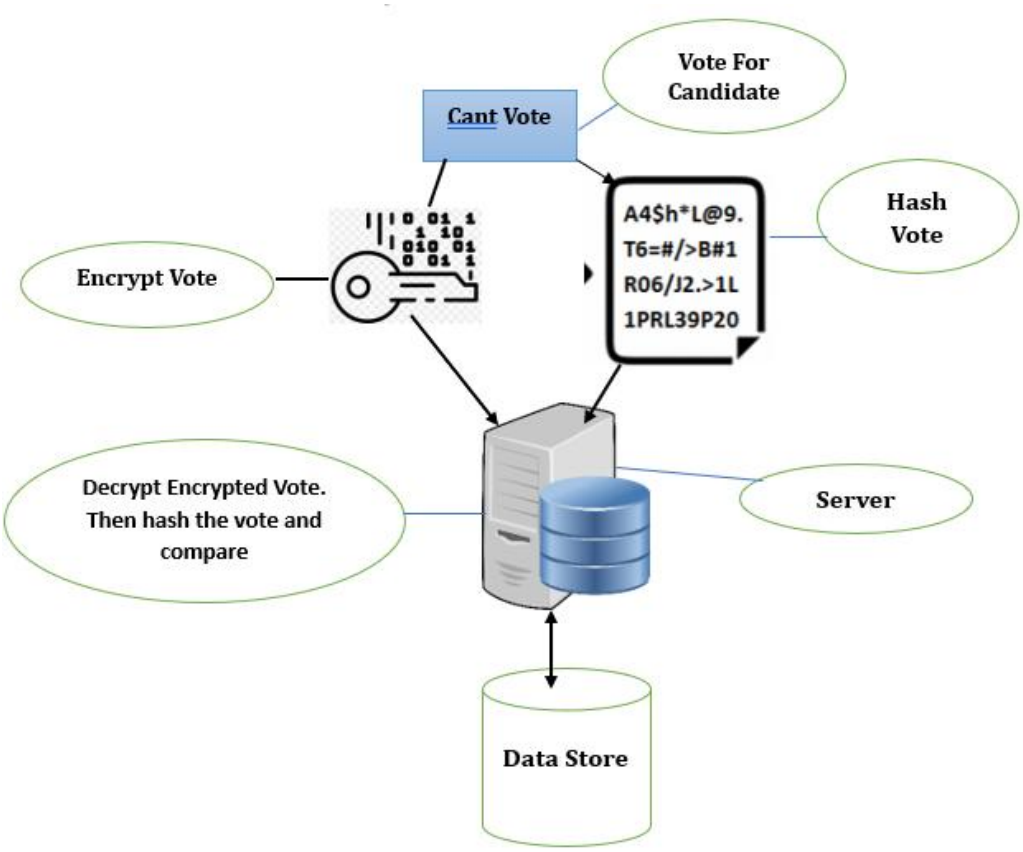


Figure 6.3: Secure E-voting Election Phase for voter's Integrity Check

The post-election phase verifies each voter's vote to ensure vote is not altered while in transit. The process involves comparing the result of each unique identity by comparing the encrypted vote to the hashed vote. The encrypted vote is decrypted and then hashed using sha256. If the hashed result matches with the hashed function sent during voting phase, the system would automatically update the user's vote by one, else, the vote would be regarded as to have been hacked while in transit, hence, vote would not be counted for the voter. Figure 6.2 shows the system flowchart of the integrity check mechanism from overall system architecture shown in figure 6.3.

C. Model Definition:

By definition, cryptographic hash functions provides assurance of data integrity with notion of implantation on fingerprint of source data, an alteration in transit of which the

integrity of data cannot longer be guaranteed. Let h be a hash function of x data, then the corresponding fingerprint or message digest is defined as:

$$Y = h(x) \qquad (1)$$

If y is stored in secure place (e.g. image or video media) then

$$k = y \qquad (2)$$

If the source data, x, is change in transit to x', then the corresponding message digest or fingerprint from equation 1 change from y= y'

$$y' = h(x') \qquad (3)$$

If data in transit has been altered by comparing equation 1 and 3, then it can be inferred that (3), y verifying that integrity of data has been compromised. The algorithm for verifying vote integrity was designed around SHA (256) as follows: Start: Vote1 = sha256 (vote) Vote2 = encrypt (vote) Vote3 = sha256 (decrypt (vote2)) Compare vote1 with vote3 If vote1 equals vote3, populate database Else return alert Stop.

Based on enhanced secure hash algorithm, message encoding and decoding algorithm below:

```
Start
AdvancedSha (String hash)
Let j, sum = 0
Let cc = empty character
While i <hash.length
 cc = hash.character(i)
 j = (AsciiFunctionOf(cc))
 sum = sum + j
 i = i + 1
end while loop
```

Output:

New hash = sha256function (sum)

Start

Let len = 100, key = 8

Encmsg ,decmsg = emptyString

Processes:

getEncode(String msg)

let i = 0;

while i <msg.length

encmsg = encmsg + msg.charactAt(i) ^ key

i = i + 1

end while

getDecode(String msg)

end

D. System Modeling:

Using Unified Modeling Language (UML) standard, the secured e-voting system was visualized along the following use case, class, sequence, and activity diagrams. The functionality anticipated by the secured e-voting system in terms of actors, their goals represented as use cases and available dependencies is shown in figure 8.

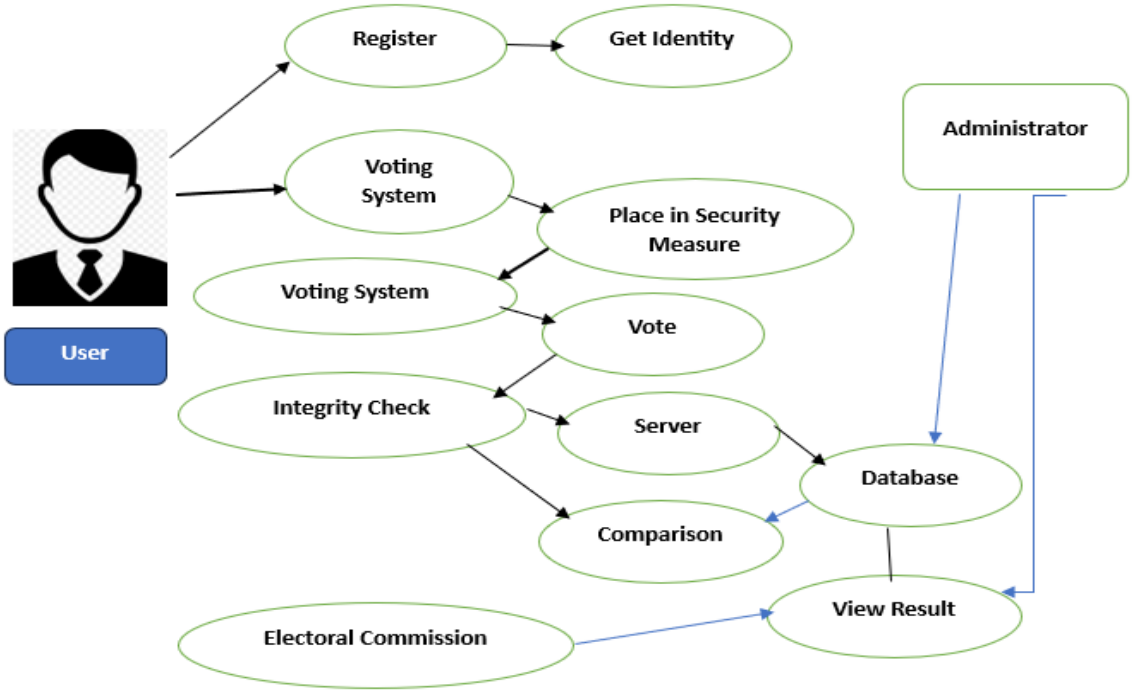


Figure 6.4: Secure E-voting System Use-case Diagram

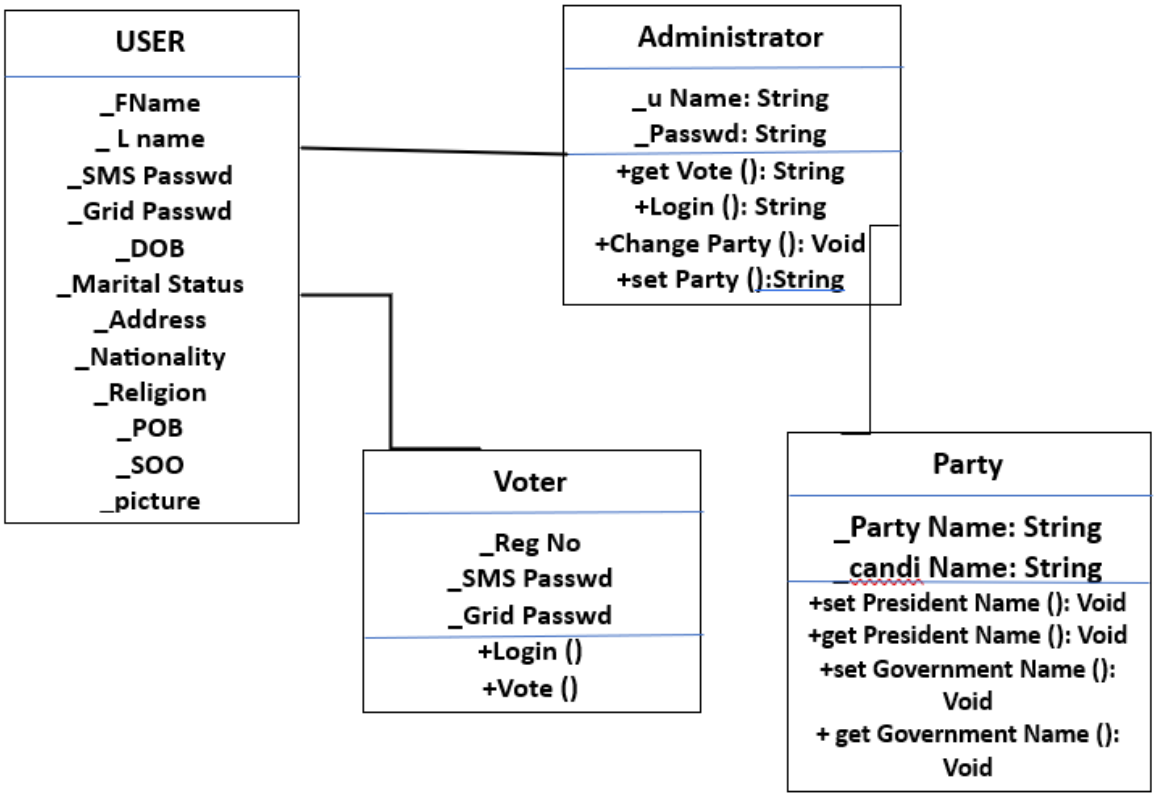


Figure 6.5: Secure E-voting System Class Diagram

System Implementation:

The hypertext processor embedded in HTML was used for the preliminary implementation of electronic web and mobile platform. The secured E-Voting system consists of two main users: the user of the system, and the administration. The administrator is the person that oversees the overall operation that takes place in the voting system. The administrative user has the right to view votes in the records, check for registered candidates, edit registered user's information, resend user's one time SMS (short message service) password, set candidates to be voted for, both in the gubernatorial and presidential election. Furthermore, the administrator has the right to disqualify a user from voting, if the registered user is not eligible to vote.

System Evaluation:

The system was evaluated through comparison of hashed vote (message digest) with encrypted vote. It displays table that represent presidential vote, having column named as Reg_Id, Encrypt_Vote, Sha_Vote, Sms_Onetime and ID. Reg_Id denotes each unique registration number of every user, whereas the Encrypt_Vote represents the casted vote in an encrypted format. The Sha_Vote represents the hashed function of encrypted vote, sms-one-time denotes that vote has not populated by the server. A figure also shows the general table of a presidential vote, and the values that are sent to the database in the server whenever a vote is made.

CHAPTER VII

ENHANCED STEGANO-CRYPTOGRAPHIC MODEL FOR SECURE ELECTRONIC VOTING

Information and Communication Technology (ICT) as a converged technology of a wide range of services and applications through various types of physical infrastructure and software systems had had a great impact on every facets of modern life. Through ICT revolution, the manner around which man share information about developmental issues has radically been affected. Government, businesses, institutions and individuals have jumped into bandwagon of adopting ICT as part of their organizational processes (Jesus, 2003). The adoption of ICT in governance is aimed at the provision of better information and services to citizens with fewer resources through optimization of available resources and infrastructures. This aim could only be achieved through effective electronic participation (e-participation) between the populace and their governing authorities (Olaniyi et al., 2012).

E-participation is a technology- mediated interaction among the citizens, formal political spheres and central governing spheres. The mission of e-participation is to endow citizen with privileges of ICT to respond in bottom-up decision processes and develop social as well as political responsibility over their choices (Dimitrios, 2011). Citizens' participation in electronic governance could be in the following context: Information provision, consultation, campaigning, deliberation, polling, electioneering and voting using different electronic methods. E-Participation through electronic voting (e-voting) is the use of ICT in the context of public voting in elections, referenda or local plebiscites. E-voting as an important e-participatory governmental service has attracted attention as cost effective and electronic decision making alternative to traditional manual method of voting (Olaniyi et al., 2013b). It is viewed as a critical constituent for improving citizen collaboration, enhance and strengthen the democratic processes in modern information societies.

Electronic voting is believed to have the capacity to engage citizens in a wider spectrum, than what is currently available in a conventional electoral process through the empowerment of citizens with a means to express their timely opinion on civil affairs such as legislation, and representation. Electronic voting has the capacity to escalate usability and accessibility of the voting process through increase in election turnout while benefiting from transparency and openness in democracy (Dimitrios, 2011).

However, the adoption of e-voting whether in physical presence or at remotes site could be vehicle for electoral fraud, if appropriate information security measures is not in place to protect electoral information, monitor voting administrators from unauthorized access, usage, disclosure, modification and destruction of vital information in all phases of electioneering processes. E-voting systems are classified as a high impact social information system, whose loss of confidentiality, integrity, authenticity and availability could have adverse effect on the credibility of near and future democratic governance (Dimitrios and Dimitrios, 2011).

Consequently, the mitigation of these insecurity threats in e-voting systems has led researchers to formulate different information hiding and privacy models. These models are designed around the principle of cryptography, steganography and watermarking. Cryptography is the science of secret writing between the source and destination while steganography is the science of keeping the existence of hidden message secret. While the former attempted data scrambling for secure communication from an eavesdropper despite his awareness of data transmission; the latter hide the existence of data transmission from the awareness of an eavesdropper for secure data transmission (Olaniyi et al., 2012). Watermarking is an information hiding technique for protection of the copyright of digital product from digital production and data safety maintenance. Its applications range from copyright image communication protection (Quan and Hong. 2008), Healthcare and

Telemedicine (Gunjal and Mali, 2012), and in secure e-voting systems (Gunjal and Mali, 2008)

In Olaniyi et al., (2013b), an attempt was made to rigorously survey existing cryptographic and stegano-cryptographic models in literatures for secure e-voting systems around their strengths and limitations. We established that the existing stegano-cryptographic models designed to provide fundamental security requirements of confidentiality, integrity, authentication and verifiability are formulated in piecemeal during pre-election phase, some proffer solution during election and post-election phase. Thus, existing stegano-cryptographic models for secure e-voting are vulnerable to attacks and can be manipulated by an eavesdropper.

An enhanced stegano-cryptographic model for secure e-voting and perform further quantitative performance assessment of the impercibility and robustness of the model using Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Root Mean Square Error (RMSE) and Structural Similarity Index Metrics (SSIM) image quality metrics as anticipated in Olaniyi et al., 2014b and Olaniyi et al., 2014c. The developed model is then compared with similar secure e-voting models in both spatial and frequency domains. An enhanced stegano-cryptographic model for secured electronic voting has been proposed for future e-democratic decision making with the view of increasing participation, confidence and trustworthiness, protects voter's against intimidation, provide sufficient evidence to convince the electorate to vote as a result of conducted, free, fair, credible and genuine e-elections.

Concept of Stegano-Cryptographic Modeling in E-voting Systems:

The notion of security in social information systems like e-voting is correlated to critical aspects of voters and ballot confidentiality, ballot integrity, voters' authenticity and voting service availability. An e-voting system is said to be unsecured, if an attacker can exploit vulnerability (a weakness) in any phase of electioneering process. To avert insecurity

in e-voting systems, researchers have formulated various steganographic techniques, cryptographic techniques and combination of both to block threats through implementation of appropriate counter measures.

While steganographic techniques ensure security by hiding voter's intent in an innocuous carrier for covert communication between the voter and voting authority; Cryptographic techniques scrambles voter's intent using an encryption algorithm for secure data communication between the voter and voting authority. In most cases, sending encrypted data over wireless channel may draw attention, while invisible communications will not draw attention (Olaniyi et al., 2012). The combination of both steganographic and cryptographic techniques for secure multilayer data communication can be used for stronger mechanism of protecting and preserving the integrity of information from an adversary (Nagham et al., 2012). The concept of stegano-cryptographic modeling technique in secure e-voting systems involved forming a hybrid technique of ensuring ballot confidentiality and integrity through simultaneous combination of covert data communication in steganography with data scrambling for secure communication in cryptography to ensure credible democratic governance. This hybrid relationship from figure 7.1 co-exists as a result of mapping between the plaintext P and Message M, Cipher Text E and Stego Media S and Cryptographic Key K and the Stego Key K. The stegano-cryptographic model results as a hybrid model with the addition of a new element: the Stego key K, giving the unifying model the cryptographic functionality while preserving the desired steganographic attributes.

The hybrid model embedding process yields Stego Media S exploiting not only Cover Media C's bits but also K's in figure 7.1.Therefore by figure 7.2, Alice (the voter) will have the privilege e to embed the secret message M (that is, the plaintext) into the Cover media C (through steganographic process) while encrypting Message M by the Cryptographic key K (Through cryptographic process) simultaneously (Olaniyi et al., 2012).

At the receiver side, Bob (the voting administrator) will be able to recover Secret Message M through Stego Media S and Stego K. In addition, Wendy (an eavesdropper) will neither detect that Secret Message M is embedded in Stego Media S nor be able to access the content of the secret message (Olaniyi et al., 2012). Figure 7.2 shows a classical example for an image based stegano-cryptographic model in e-voting systems. For instance in image steganographic application, the integrity of a voter and his vote is assured with the encryption of the message (vote) and then embedding of the encrypted message inside a 24-bit cover image.

A secret key used for the stego-system encoder is then passed through the communication channel. At the voters administrator end, the secret key is used to extract the hidden message from the stego-image as shown in figure 10.

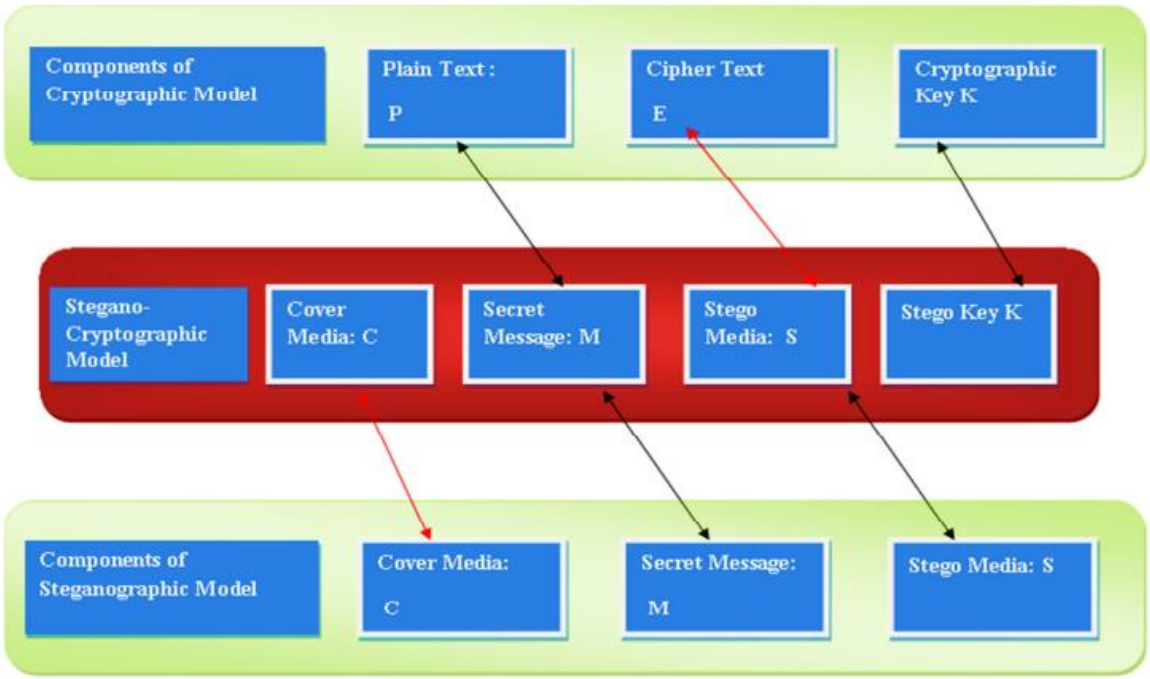


Figure 7.1: General Stegano-Cryptographic Model Mapping from Steganography and Cryptography (Adapted from (Bloisi and Luca , 2007))

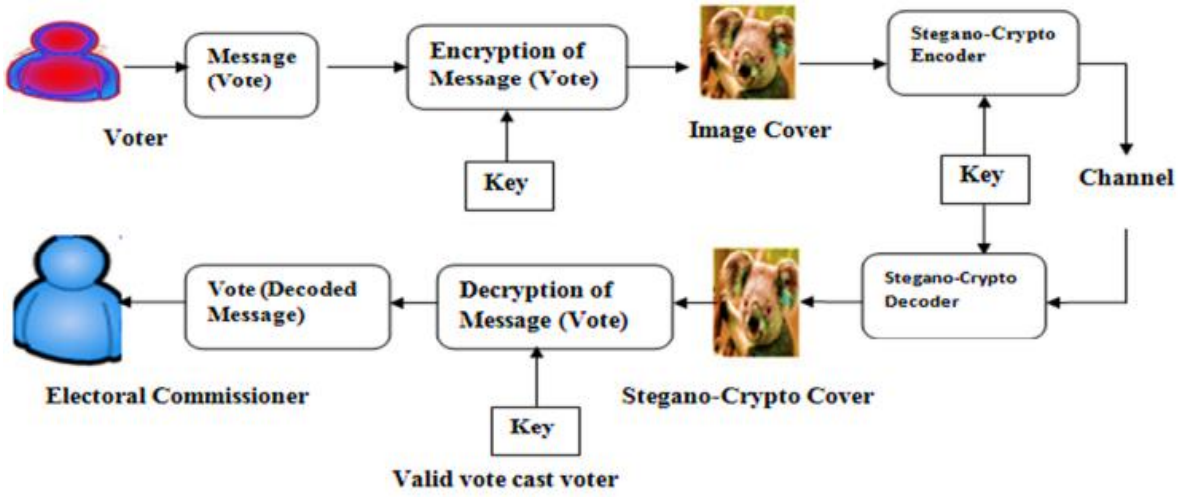


Figure 7.2: Application of Stegano-Cryptographic Modeling Technique in E-voting (Olaniyi et al., 2012)

Secure E-voting Model:

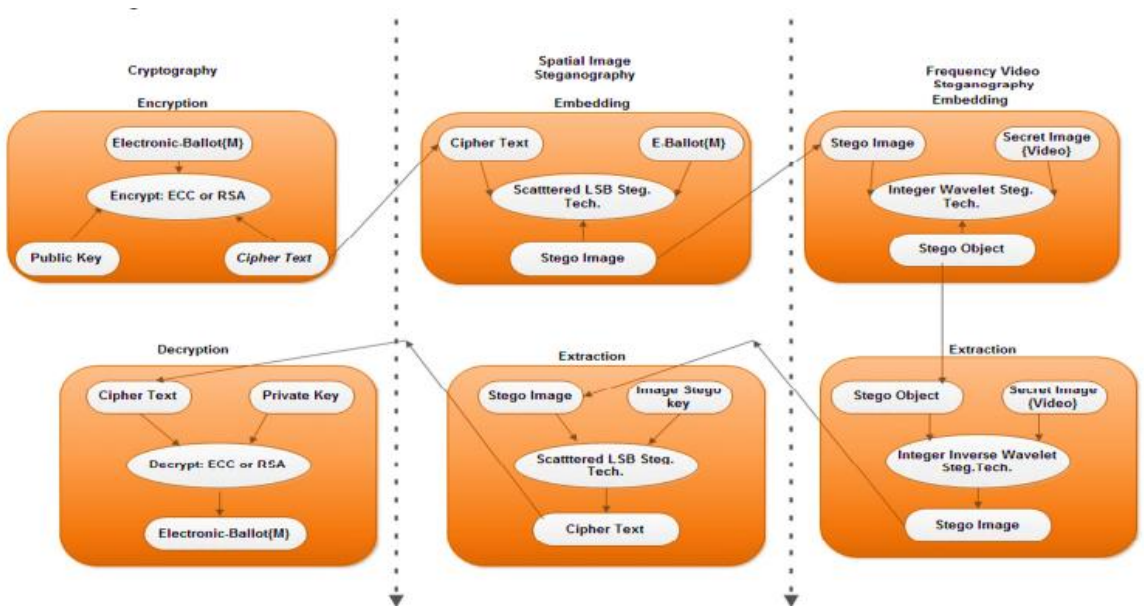


Figure 7.3: Enhanced Stegano-Cryptographic Model of Secured E-voting Olaniyi et al., (2014c)

The enhanced model for secure e-voting shown in figure 7.3 improves on katiyar et al., (2011) unimedia stegano-cryptographic model by encrypting electronic ballot using Elliptic Curve Cryptography and Rivest Sharma Adleman cryptographic algorithm. The encrypted voter's ballot was scattered and hidden in the Least Significant Bit (LSB) of the

cover media using information hiding attribute of modified LSB-Wavelet steganographic algorithm in both spatial and frequency domain for multilayer(steganography and cryptography), multimedia(Image and Video) and multi-domain (spatial and frequency) secure e-voting modeling for future e-democratic governance

As shown in figure 7.3, the approach of our image steganographic technique was the modified Least Significant Bit (LSB). The technique consists of two parts namely the embedding and the extraction part. The developed algorithm takes the LSB of the cover medium (Spatial Image) and swaps them with a sequence of bytes containing binary equivalent of voters confidential information (electronic ballot). Although, the hiding capacity and impercibility of traditional LSB technique is low considering the statistical features of the stego image in comparison to the original image. The developed embedding algorithm employed modified LSB technique by scattering the bit equivalent of electronic ballot in random bits of the cover image in order to embed the confidential voter's intent.

The bit of the cover image to be used for steganography is first extracted to allow for the hiding of the byte values of the text strings randomly in the byte values of the image. To fulfill this objective, the multiplicative congruential random number generation technique was used to generate sequence of random numbers used to match the specific bits in the cover image where the secret bit- electronic ballot are to be hidden. The multiplicative congruential method is an arithmetic procedure to generate a finite sequence of uniformly distributed random numbers. Two integers P and Q are congruent, if their difference is an integral multiple of m.

Embedding Algorithm

These steps were transformed to embedding algorithm as:

Input: Cover image C, Ciphered message M,
Output: Stego image S
Let LSB(C_{ei}) =M_i (M_i can be either 1 or 0).
For i =1 to Length (M) Do
Get random pixel of cover elements such that $\{e_1, e_2, \ldots . e_{1m}\}$ using MCRG
C_{ei}=M_i←LSB (M_i) // Replace C_{ei} with the i^{th} message bit of M in computed random pixel of cover image
End for
S = C_{ei}

Extracting Algorithm

The general procedure of extracting encrypted as well as hidden vote is:

1. Begin
2. Read the stego image, S.
3. Calculate LSB of each pixels of stego image.
4. Retrieve cipher text bits
5. Pack the retrieved bit into character.
6. End

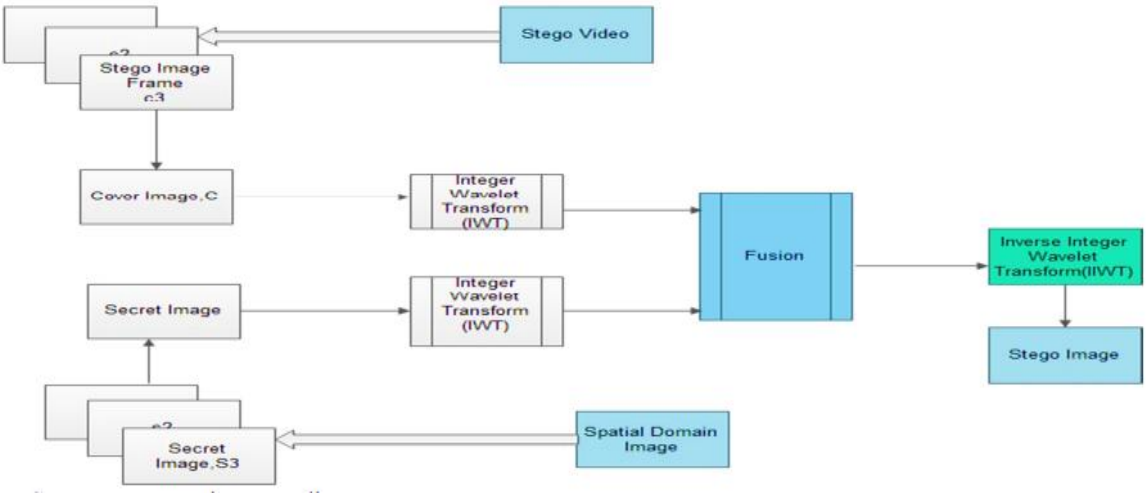
The extraction algorithm from above procedure thus is:

Input: Stego-image S
Output: Ciphered Message M
For i =1 to Length (M) Do
M_i = C_{ei}LSB (C_{ei})
End for

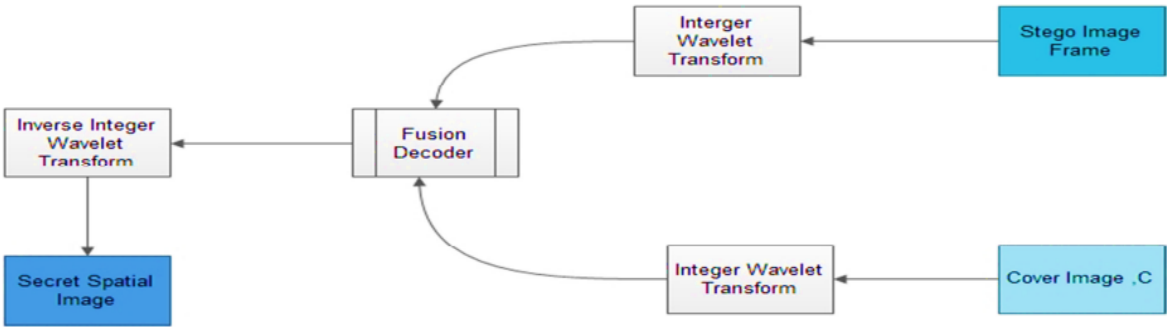
The integer wavelet transform (IWT) approach of frequency steganographic technique was used based on the merits reported in Chedad et al., (2008): Hidden messages perceptually invisible, statistically undetectable and difficulty in payload extraction during transit. In order to prevent loss of payload hidden in the stego image in spatial domain, an invertible integer-to-integer wavelet transform (IIWT) is adopted for video frequency steganography. Figure 7.4 a shows the embedding process of merging wavelets decomposition of the normalized version of the cover image (from sample video frame) and secret image (spatial stego image) into single fused result (stego video), the payload. Both cover image and secret image are transformed into IWT domain. Further application of IWT on the payload increases the security level. The single fused resultant matrix is obtained based on the addition of wavelet coefficient of the respective sub bands of the cover images and secret image.

The first step of IIWT on these coefficients is applied by second IIWT in order to retrieve the coefficient of the secret image P as shown in Figure 7.3. The extraction algorithm at wavelet transform domain thus is: Input: Stego Image frame, S. Output: Payload, P, spatial stego image.

- Step 1: Get the stego image frame S as the input to the decoder.
- Step 2: Apply the IIWT for the original cover image and the stego image.
- Step 3: Subtract IIWT coefficients of cover Image, c from IWT coefficients of stego image frames to get the IWT coefficient of only p.
- Step 4: Apply IIWT to all sub bands of payload P Step5: The secret spatial image P is obtained.



a: Stego Image Fusion encoding process



b: Stego Image Fusion decoding process

Figure 7.4: Stego object fusion encoding and decoding process (Olaniyi, et al., 2014c)

Voting Procedure:

In manual paper based voting, the procedure for an election involves, registration, accreditation of voters, voting, collation of ballots, counting and announcement of election results. Similarly, in secure e-voting systems similar procedure is observe with implementation of different information system security techniques and protocols unique to individual proposition. The following steps are the procedure involved in our proposed enhanced stegano-cryptographic based secure e-voting system.

Registration Phase:

The registration stage is the planning stage for preparation towards possible constraints in the entire phase of electoral process. The right of the voters to vote was ensured only eligible voters can accurately cast a vote after successful voter's registration. Each voter would be identified through multifactor authentication: what the voter has (One time pin password), what the voters is (biometric fingerprint) and what the voter accurately respond to (Visual Challenge response to Grid questions) in kiosk, poll sites and remote e-voting scenarios.

Authentication and Validation Phase:

Since the model considers e-voting from the lens of kiosk/ poll-site, web and mobile voting scenarios, registered voters would be required to input their unique credentials based on the platform of voting. For kiosk/poll site evoting scenarios, voters would be authenticated through enrolled credentials of one time pin password, biometric fingerprint and accurate response to visual challenge to real time grid questions. The remote e-voting procedure would be authenticated and validated through one time pin password and accurate response to visual challenge to real time grid questions for proper level of trust between the voter and the system. The voter would be privileged to vote immediately their credentials are authenticated and validated as who they claim they are.

Voting Phase:

This embraces the selection of voter's candidate by the voter as well as the process of sending the electronic ballot to the server. Our enhanced model for secure e-voting presented in section three for electronic ballot scrambling and embedding in image and video cover both in spatial and frequency domain are used protect the voter's intent as stego object from an eavesdropper or an attacker for kiosk, poll sites and remote e-voting scenarios. This process is shown in UML activity diagram of enhanced stegano-cryptographic model for secured e-voting of figure 7.5 in figure 7.6.

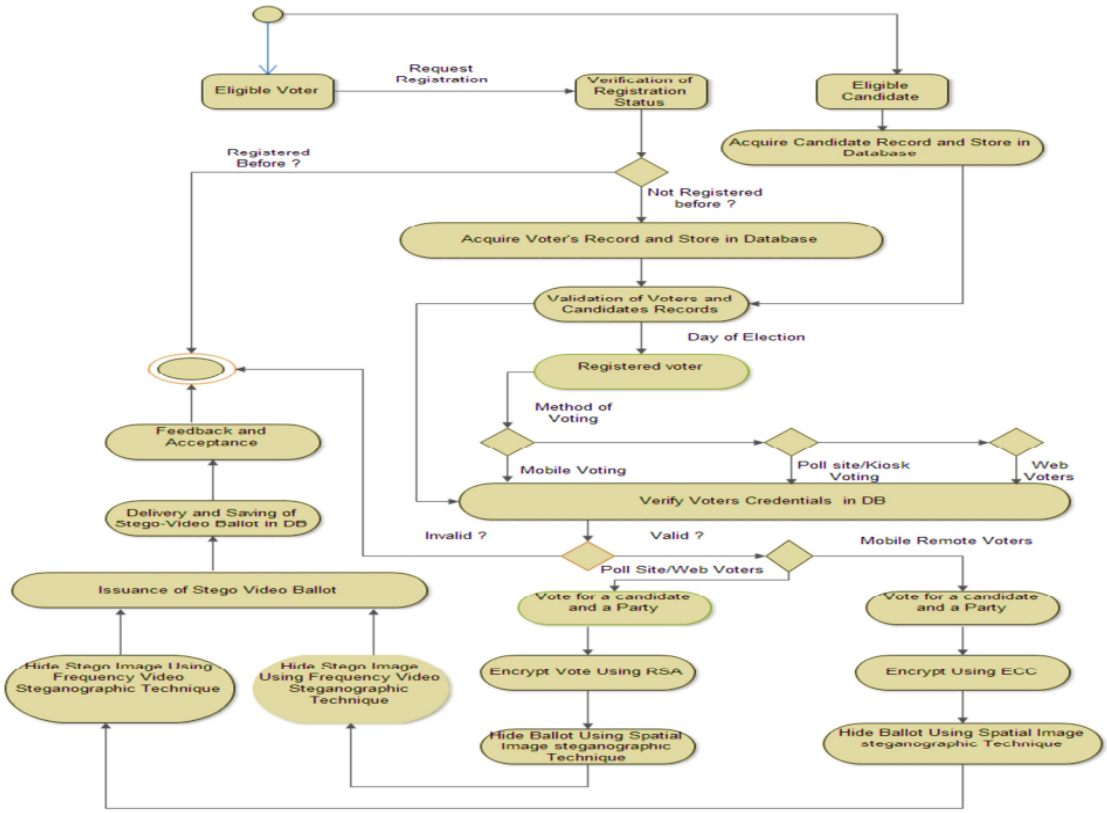


Figure 5: UML activity diagram of enhanced stegano-cryptographic model for secured e-voting in Figure 3 (Olaniyi, *et al.,* 2014c)

Tallying:

In this stage, each collected electronic ballot technically referred to as stego object, is first extracted using the wavelet steganographic algorithm to yield a stego image. The stego image is further processed with LSB steganographic algorithm to yield an encrypted cipher

text containing the hidden electronic voter bit for extraction using either RSA or ECC depending on the platform of voting. The extracted votes are then collated by an administrator for publication to the electorate.

Publishing and Ballot Verification:

In classical paper based voting, the announcement of the result of the election succeeds the tallying process. In secure e-voting system based on our enhanced model, the integrity of extracted vote while in transit is ensured by validating an altered vote during transit at the post-election phase by encoding the vote with a private key. The process involves comparing the result of each electronic ballot by comparing the encrypted vote added the ballot to the hashed vote.

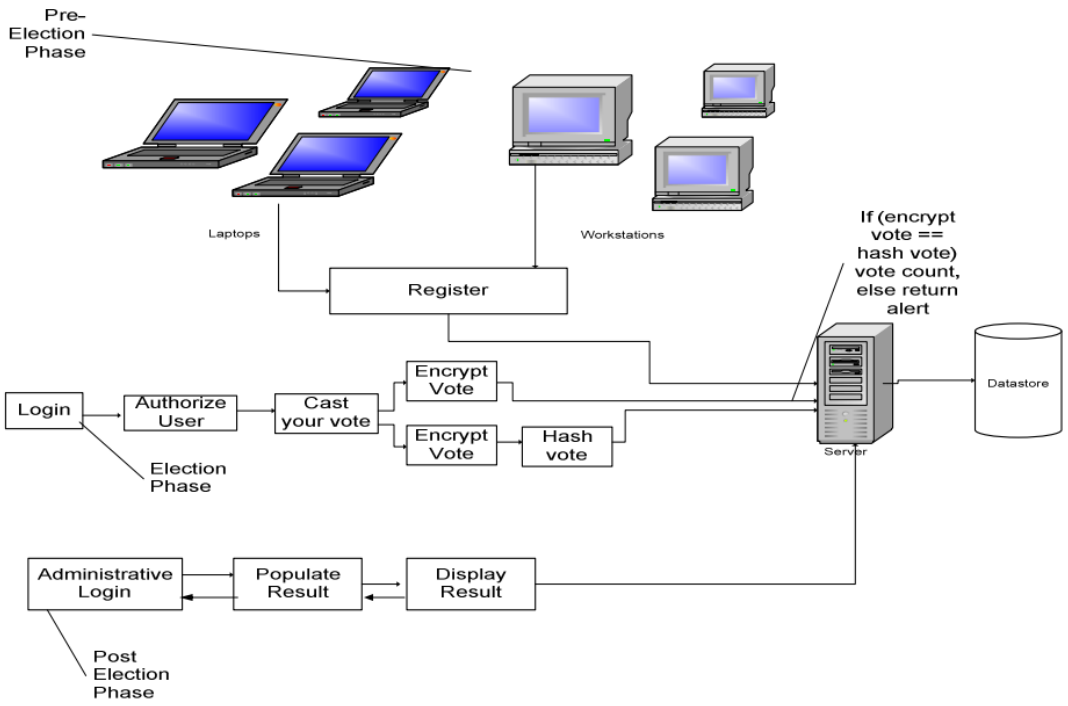


Figure 6: Vote Integrity check of extracted electronic ballot (Olaniyi, *et al*., 2013a)

The encrypted vote is decrypted and then hashed using SHA256 hashing algorithm. If the hashed result matches with the hashed function sent during voting phase, the system (the server) would automatically update the user's vote by one, else, the vote would be regarded as to have been hacked while in transit, hence, vote would not be counted for the user (Olaniyi,

et al., 2013a). This ballot integrity procedure is shown in Figure 7.6. Also, voters can also secretly verify whether their vote is among the collated vote for final declaration of result.

In this manner, the fundamental security requirements of authentication, integrity, confidentiality and verifiability has been achieved as neither the voters nor the election administrator has access to identify the collected electronic ballots.

System Implementation:

The model was simulated using JAVA Programming Language and Oracle 10g Database Management System (DBMS). Selected qualified voters were asked to enroll data for remote mobile e-voting scenario through interaction with the sample secure e-voting system Graphical User Interface (GUI) presented in figure 7.7. The detailed system implementation of the enhanced model for both kiosk and poll- site e-voting scenarios have been presented in Olaniyi et al. (2014c). The system (GUI) of the mobile voting system based on the developed model required the voters to enroll their unique physiological biometric fingerprint, their personal data during registration phase prior to voting using their mobile devices.

Model Performance Evaluation:

The performance measure of steganographic systems are measured along three key parameters: imperceptibility, robustness and payload capacity and the stability of the stego media against detection using steganalytic detectors (Nagham et al., 2012; Olaniyi et al., 2014b; Olaniyi et al., 2014c).

These three key parameters are defined as:

- Imperceptibility: The ability to avoid detection i.e. where the human visual fail to notice it. Impercibility parameter is the primary requirement of a steganographic technique. Truly secure steganographic technique should be imperceptible neither by human eye nor by statistical attacks (Nagham et al., 2012).

- Robustness: This is the ability of steganographic technique to survive the attempts to remove the hidden information through attempts like cropping, rotation (in cover medium like image), data compression and filtering.
- Payload Capacity: Payload refers to information that can be hidden in cover media during steganographic process. Payload capacity therefore refers to the maximum amount of information that can be hidden and retrieved successfully.

Performance evaluation of our enhanced model was accomplished both quantitatively and qualitatively. Quantitatively through computation of SSIM stego image quality metrics value for different stego image pixel dimensions using ImageJ, Image processing environment. Qualitatively using five-point likert psychometric analysis, descriptively analysed in Statistical Package for Social Sciences (SPSS) through assessment of users perceptive of secure e-voting system based on the developed stegano-cryptographic e-voting technique. In Olaniyi et al., 2014a; Olaniyi et al., 2014b and Olaniyi et al., 2014c preliminary quantitative and qualitative performance evaluation of our model have been carried out respectively. In this section, further quantitative performance evaluation of the confidentiality requirements of secure e-voting model was evaluated based on assessment of stego image quality. The assessment the quality of the developed model stego Image was accomplished through computation of Root Mean Square Error (RMSE), Signal to Noise Ratio (SNR), Peak to Signal Noise Ratio (PSNR) and full referenced multi-indexed Structural Similarity Index metrics (SSIM) between the distorted image - the stego image and its reference image cover image for index levels of 0 to 3 using SNR and SSIM plugin in ImageJ Image processing environment.

ImageJ program is a Java based Image processing application for editing, analysing and processing color and gray scale Images. Our findings of the assessment of the stego Image quality (shown in Figure 8) using RMSE, SNR,PSNR and full referenced, multi-index

Structural Similarity Index metrics (SSIM) between the distorted image (stego image) and its reference image cover image is shown in Table 1. Considering SNR and PSNR similarity metrics in Table 1, increase in security of multilayer and multi-domain e-voting model is inversely proportional to image size, with both values of PSNR and SNR increasing with decrease in pixel value of image. This signifies the e-voting model is secured from theoretical perspective: high PSNR value indicates high image quality.

A: Cover Image (8-bit, Grayscale)

B: Stego Image(8bit Grayscale)

Figure 8: Cover and Stego Image in Grayscale.

Table 1: Comparison of various quality measurements on stego image and cover image

Cover Image	Stego Image	SNR[dB]	PSNR[dB]	RMSE [dB]	SSIM(at level 0)	SSIM(at level 1)	SSIM(at level 2)	SSIM(at level 3)
Bellslogo.jpg 512*512	Bellslogo.jpg 512*512	50.118	56.015	89.136	0.7706	0.5700	0.7214	0.7698
Bells logo.jpg 256*256	Bellslogo.jpg 256*256	51.909	57.840	83.109	0.8179	0.7191	0.7504	0.8011
Bells logo.jpg 128*128	Bellslogo.jpg 128*128	55.569	61.566	72.030	0.8989	0.8075	0.8457	0.9056
Bellslogo.jpg 64*64	Bellslogo.jpg 64*64	63.963	70.097	50.025	0.9459	0.8847	0.9185	0.9569

Also, considering the limitations of PSNR, SNR and MSE image quality metrics: Inability to assess effectively image similarity across distortion types and inability to matched perceived visual quality (Vincent and Adepoju 2013; Mittal, et al., 2013; Wang et al., 2004), necessitated the computation of full reference Structural Similarity Index metrics (SSIM) at index level of 0 to 3 of the stego image in Table 1. According to Aibinu et al., (2008), For two images x and y of common size N*N, SSIM is given as:

$$SSIM(x,y) = ((2\mu_x\,\mu_y\ + C_1)(\,2\sigma_{xy} + C_2\,))/((\mu_x^2\ + \mu_v^2\ + C_1\,)(\,\sigma_x^2 + \sigma_y^2\ + C_1\,)) \quad (6)$$

$$SSIM = [-1, +1] \quad (7)$$

The best value 1 is achieved if and only if the two images are similar and -1 if the two images are highly un-similar (Aibinu et al., 2008). From equation 7, the increase in index value from 0 to 3 made computed SSIM value to 1 (from 0. 0.8989 to 0.9056 in Bellslogo.jpg of 128*128) indicating greater fidelity of stego image closeness to the original cover image, hence the developed e-voting model is imperceptibly secured.

Comparative Assessment with Other Similar Models of E-Voting Systems:

The developed enhanced stegano-cryptographic model for secure e-voting was compared with other existing methods in literatures, in spatial domain like Rura et al., 2011,Katiyar et al., 2011, and Prabha and Ramamoorthy (2012),Kamau et al.,2013 and in transform domain like Shamin and kattamanchi (2012). From the comparative study, it can be concluded that the developed e-voting model is better in terms of high impercibility of stego image, high robustness to survive attempts to remove the hidden data, moderate PSNR values and qualitative SSIM values compare to existing stegano-cryptographic e-voting model in literature. Table 2 and Table 3 show the comparison of the developed modified stegano-cryptographic model for e-voting with other existing e-voting model in different domains. Table 4 shows the numerical comparison of PSNR metric values with existing e-voting models. The developed model is 37.58% and 16.14% better than Shamin and kattamanchi (2012) and Kamau et al., (2013) in frequency and spatial domain respectively.

Table 2: Comparison of the developed e-voting model with other spatial domain method

S/N	Paramater of Comparison	Rura *et al.*, 2011,Katiyar *et al.*, 2011, Prabha and Ramamoorthy (2012) and Kamau *et al.*, (2013)	The developed e-voting model
1	**Attack on Image**	Because all are e-voting model based on spatial domain techniques.,data are easily easily tractable from raw pixel intensities and falter for most types of image attacks.	Since the model embraces further transform domain layer on the spatial stego image using wavelet techniques, extraction from wavelet coefficients is far more complex and robust with chosen jpeg image.
2	**Image compression factor**	All e-voting models embraces only uncompressed image	The model works on both uncompressed and compressed image.
3	**Performance evaluation factor**	Rura et al evaluated only with histogram level;Katiyar et al and Prabha and Ramamoorthy (2012) evaluated only with the speed of hash function which cannot effectively established the security of the scheme for e-voting.	Model was evaluated qualitatively with RMSE, SNR,P SNR and SSIM standard image quality metrics with high level of imperceptibility index rate and quantitatively with pyschometric analysis with high rate of user's perceptive rating.
4	**Test of the hidden data security**	Secuirty of the idden data not tested.	Security of tested hidden data using steganalysis was very high.

Table 3: Comparison of the developed e-voting model with other DCT domain method

S/N	Paramater of Comparison	Shamin and kattamanchi(2012)	The developed e-voting model
1	**Method of transformations**	The model embraces transform domain techniques by modifying DCT coefficients.	The developed evoting model embraces the modification of both scattered LSB spatial image and wavelet frequency coefficients.
2	**Image compression factor**	The model works only on uncompressed image	The model works on both uncompressed and compressed image.
3	**Security of hidden data**	Security of the hidden data tested with PSNR metric	Security of tested hidden data using steganalysis and SNR,PSNR and SSIM Image quality metrics

Table 4: Numerical Comparison of the PSNR Metric values of the developed e-voting model with other Exiting E-voting Models/Technique

S/N	Similar E-voting Model/Technique	PSNR Computations(dB)	Percentage of Comparison (%)
1	Kamau, Kimani and Nwangi (2013)	58.78	***16.14***
2	Gunjal and Mali (2012)	54.32	***22.50***
3	Shamin and kattamanchi (2012)	43.75	***37.58***
4	Mallick and kamilla (2011)	42.77	***38.98***
5	The developed Model	**70.09**	

CHAPTER VIII

A NOVEL HYBRID BIOMETRIC ELECTRONIC VOTING SYSTEM

Electoral Systems empower the citizens of a country to elect parliament members of their choice. Paper based electoral system is a classical method to accomplish the said task. In this method, printed votes are submitted to various election booths of country at least one day before the election. After the election timings, sealed boxes containing votes are opened in front of all the legitimate members of booth and counted. The information of counted votes is submitted to a centralized station along with bags of paper votes.

The central station compiles and publishes the names of winners and losers through television and radio stations. This method is useful only if the whole process is completed in a transparent way. However, there are some drawbacks to this system. These include higher expenses, longer time to complete the voting process, fraudulent practices by the authorities administering elections as well as malpractices by the voters [41]. These challenges result in manipulated election results. Electronic Voting Systems provide efficient and reliable technique to empower citizens of a country or members of an organization to select a person of their choice. These systems can be classified into supervised, hybrid and remote voting styles. Supervised voting also known as offline voting is typically administered by electoral organizations.

In this scheme, voting machines are located at polling machines. However, these machines are not connected with a centralized system for cross-verification or any other purpose. Hybrid voting schemes are supervised by election organizing members, however, the machines are connected with internet, Remote voting refers to the schemes which are not administered by any supervising staff and the machines are connected with internet [42]. Benefits of using Biometrics in a voting system is to accurately recognize the voter which

enables the election administrators to reduce the error rates by reducing fraudulent and bogus votes.

Besides, it also results in cost efficiency, improving physical safety and increasing convenience to the users [46] In this regard, various authors have developed the electronic voting systems. A smart card based voting system is developed by [44]. This smart card system has temporary and permanent storage facilities. To address fraudulent practices, this card also contains biometric information of the end user which can be authenticated by the system. Sehr [45] present a computerized voting system to address issues including low attendance of voters, higher administration and operation costs, longer time of tabulation, and inconvenience for voters, rigid voting guidelines, and inadequate security protection. Tagawa [6], present an innovative electronic voting system.

The proposed system encodes voting information. This system consists of voting unit, polling administration unit, voter list administration unit and ballot or counting unit. After the vote is caste, the information is sent to polling administration unit along with the smart card number in encrypted manner. During the comparison if the information is found to be doubtful the vote will be rejected. Otherwise it can be preceded to the ballot counting unit. It is an effective system with proper data encryption and secrecy but it lacks one feature i.e. multiple votes by a single user. Evertz [47] presents a system using WAN (Wide Area Network) which is connected to a server at the election office containing the database of all the voters. First the voter has to verify its identity by facial recognition, in which features are extracted from the face of the voter and compared with pre-stored features in a database.

Upon matching of the identity, a window will pop up on the screen of the computer where the voter can cast its vote. But the facial recognition system used and employed is quite in-effective having a success percentage of only 58% and a response time of 15 seconds. Besides, it lacks any data encryption or security for the secrecy of the ballot. Thus rendering it

in-effective for use in real-time. To improve the confidentiality and privacy of the electronic voting systems, most of the systems use Mixnet or homomorphic encryption techniques [48].

Additionally, authors also claim that the homomorphic encryption is more appropriate for the situation with several election candidates as well as elections with neutral votes. The electronic voting system is implemented extensively in developed countries such as USA. Awad and Leiss [9], present a comprehensive study of conventional and electronic voting systems in USA along with their disadvantages. Alomari and Irani [10], present e-voting for a developing country, hence they concluded that the factors that Influence the adoption of e-voting includes trust in internet, trust in government, attitudes, website design, and compatibility including many others. Pesado et. al. [49], have presented the challenges and solutions of electronic voting system preferably for Argentina.

Additionally, they have presented the characteristics of three different voting types, these include on site electronic voting system, partially onsite and remote voting system. Furthermore, policy considerations are also provided for the implementation of the proposed system. Jacobs and Oostdijk [42], present a system that uses bar coded identifiers which are assigned either randomly or pseudo randomly in the form of combination of numbers and alphabets. These encrypted codes provide security from any illegal intervention. Using different identifiers makes this system secure in comparison to others. The voter will then have to scan the bar-code and then the system will decode and compare the code assigned with that of the database.

Upon a perfect match the voter will be allowed to vote. Awan et. al. [43], implement a fingerprint based electronic voting system using Raspberry Pi board. Vidyasree et. al. [44], fuse the fingerprint and facial data to improve the identification of a voter through multimodal system. The results show a reasonable amount of improvement in comparison to unimodal

system. Das et. al. [50], store biometric information of the user i.e. fingerprints on RF ID tags for designing an improved electronic voting machine.

The proposed system also integrates the GSM module to disseminate information from the local station to other stations. We develop and present an electronic voting system to eradicate fraudulent practices during public elections by involving double user identification checks i.e. facial recognition and finger print based identification methods.

Facial recognition is accomplished through a feature-extraction based machine learning algorithm, while finger print based identification is achieved through pattern recognition method. The facial recognition is accomplished through cascading of Global Principal Component Analysis and K nearest Neighbor algorithms. The proposed method will provide better accuracy in comparison to a single identification method.

The Proposed System:

In this section, a brief description of various hardware units is presented that are integrated in proposed project to achieve the improved results for the proposed electronic voting system, as shown in figure 1. Microcontroller: A microcontroller can be defined as an integrated circuit that contains a core processor and memory 416]. Microcontroller is also known as an embedded system, capable of storing, processing and transferring data and information between various peripherals interfaced with it on some logic, i.e. like a coordinating body of a circuit. With the advancement in the field of electronic technology especially in microelectronics and embedded system development, various development boards are available. These boards include Arduino-UNO, Texas Instruments MSP 430 Launchpad, Nanode, Pinguino PIC 32, Teensy 2.0, Raspberry Pi and many others. These boards not only provide microcontroller facility to the end user but also an interfacing capability to connect different devices i.e. Bluetooth, Zigbee, LAN and WLAN (Wireless LAN also called WiFi). The proposed system (in our research) uses Arduino-UNO board due

to good processing speed as well as memory, and capable of interfacing, controlling and monitoring of data flow [47].

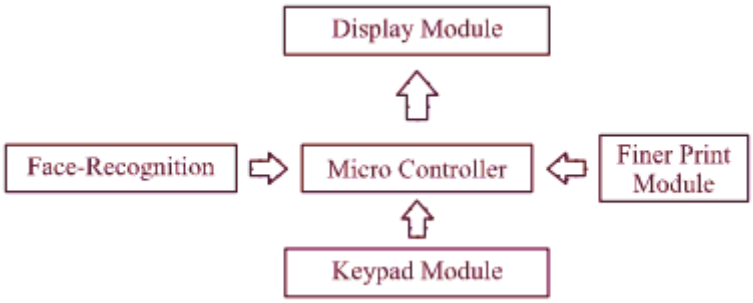


Figure 8.1: Block Diagram of CR Based Biometric Electronic Voting System

Fingerprint Module: Unique finger impression recognition or fingerprint authentication indicates the mechanized strategy for checking a match between two human fingerprints [38]. The examination of fingerprints for coordinating purposes requires the correlation of components of the print design. The extracted parameters of a finger pattern include edges and minutia focuses [39]. These distinct features of a biological pattern give uniqueness to a human being.

The mechanized method for the verification of a fingerprint is done by using an electronic device called Fingerprint Verification Module, which captures the unique pattern of a fingerprint in the form of a computerized digital image. The digitally captured images are then processed to prepare a biometric template. This biometric layout is an accumulation of extricated elements which is stored and utilized for coordinating and matching [40].

The proposed system uses a finger print verification module developed by Future Electronics Egypt. Facial Recognition System: Facial recognition system or facial acknowledgement framework is defined as an application capable of detecting and recognizing a person from a digitally processed image [41]. This unit comprises of facial recognition algorithms which includes facial detection, facial feature extraction, formation of biometric template by compression and formation of Eigen vectors and their comparison.

Many popular facial recognition algorithms are available in literature that include PCA (Principal Component Analysis) using Eigen faces, LDA (Linear Discriminate Analysis), Fisher-face algorithm and Dynamic link matching [42]. The proposed system incorporates the facial recognition algorithm, developed by [43]. The details of the algorithm and its working details are provided in the next section of this paper. A flow diagram of the proposed algorithmic setup is shown in figure 8.2.

Figure 8.2: Block Diagram for Face Recognition

The input image is processed to be utilized by trained classifiers that produce a final decision of either recognized or unrecognized.

Working Procedure:

In this section, a brief working procedure of biometric data extraction and processing is presented. Figure 8.3 shows the registration steps to be taken for the new voter registration into the proposed voting system. Figure 8.3 shows the execution process of the proposed electronic voting system. As shown in figure 8.3, the registration of the voter begins by the start of the counter for assigning a voter number to each voter. The message is displayed on the screen to place the face in front of the camera, the image is captured and normalized and divided into 24X24 sub-windows. Thus, distinct features are extracted and a vectored biometric layout of the facial image is formed.

The resulting biometric template can be used to train the classifier using Adaboost trainer and then a codebook for the Eigen vectors is formed, then the generated biometric layout is saved in the database against the encrypted ID number. This ends the first step towards recognition of facial features. Then a message is displayed to place the thumb on the

scanner, the thumb sensor scans and forms a biometric layout of the thumb of the voter and stores it against the same encrypted voter number in the database.

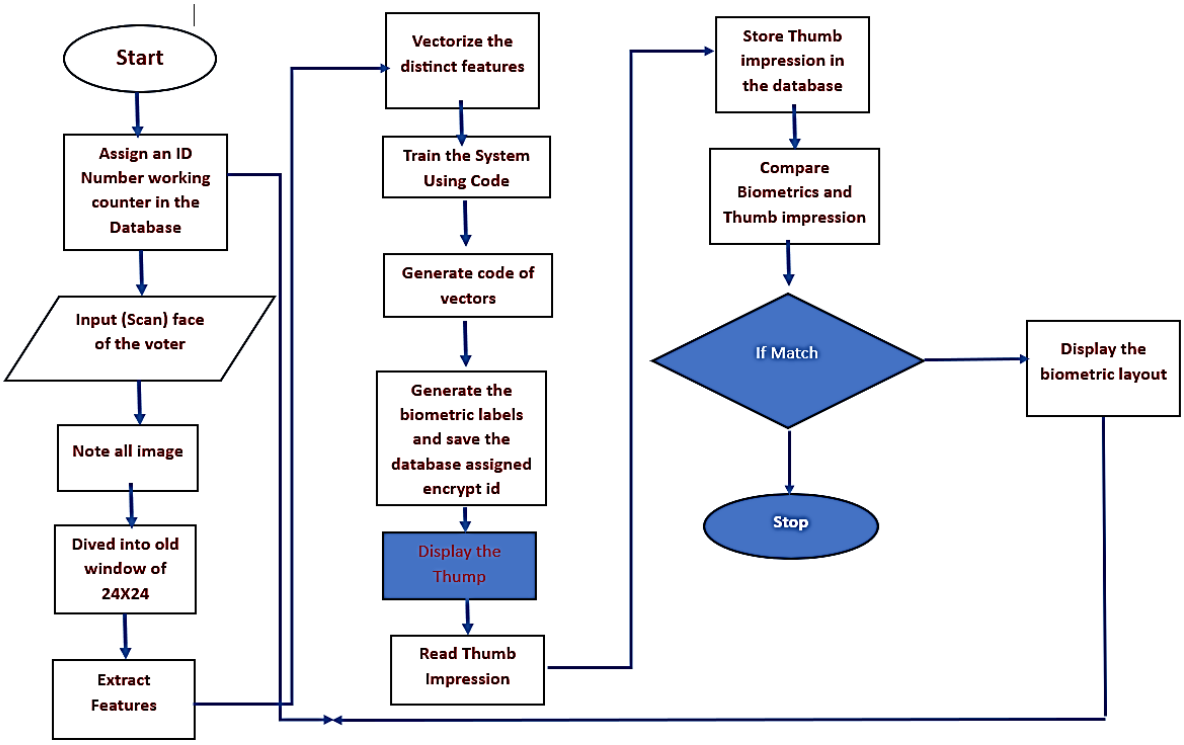


Figure 8.3: Showing the Registration Process of Voter

Now both facial and thumb print biometric templates are compared with the pre-stored biometric layouts in the database in order to eradicate registration of the same voter multiple times. In case the registered voter tries to repeat the registration step again, the registration is rejected. During the voting process, a message is displayed to place the thumb on the thumb sensor/scanner; a biometric layout is generated and is compared with the database in order to find a match. In case the thumb impression is not found in the database, an error is displayed and a message is generated for the relevant users. In case a match is found, a message is displayed for the voter to place the face in front of the camera. The image is then normalized, 24X24 sub-windows are formed and features are extracted. The distinct features are vectored and are then compared with the biometric layout in the database. If a match is found, the voter is allowed to cast the vote. But in case no match is found, an error is displayed and a message is generated to the relevant authority, as shown in figure 8.4. In this section, the detailed

process of the individual steps is presented. Facial Recognition System: The facial recognition system is the most significant feature of the proposed hybrid biometric electronic voting system. The algorithms used for facial recognition usually can be categorized into two methods firstly geometric which compare the geometry of distinct features and analyze the relative position, size and shape of ears, eyes nose and jawbones and secondly photometric which is a statistical methodology to distill a picture into statistical values and compares the values with the layout [24]. The algorithm used in the proposed system is based on the principle of feature extraction. Feature extraction in image processing may be defined as being a set of initial value derived from an object in the form of a pattern which is informative and useful for machine learning.

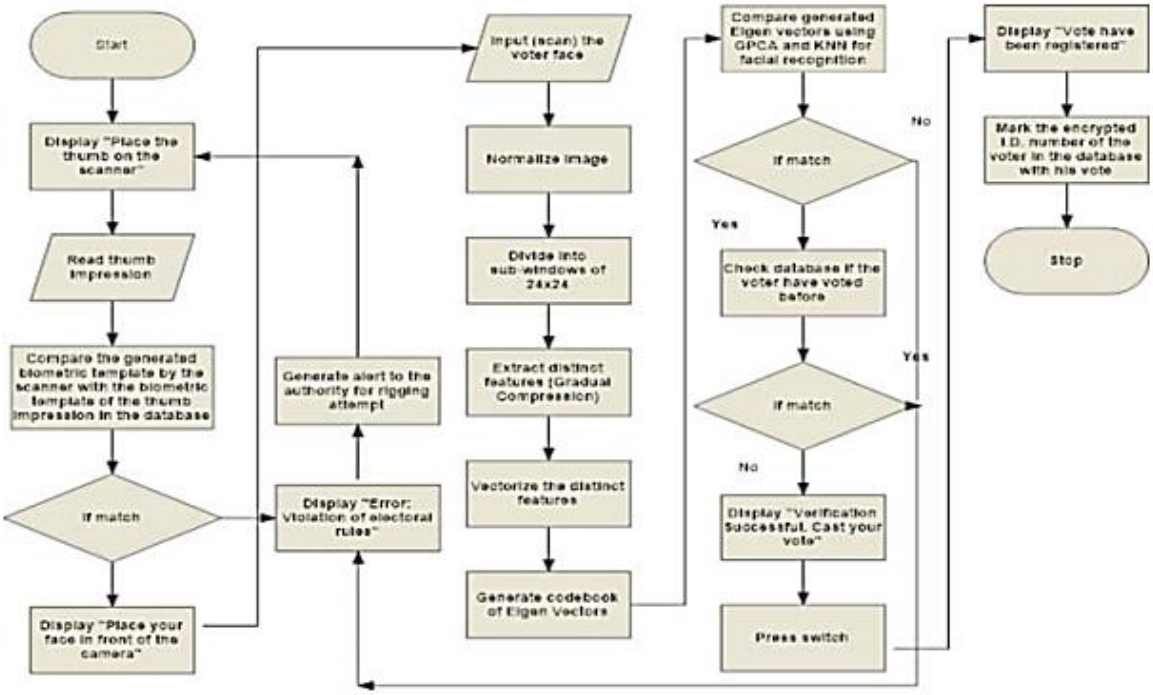


Figure 8.4: Execution Process for Proposed Electronic Voting System

The algorithm can be implemented using three steps i.e. Haar feature selection, creation of an integral image and Adaboost training [45]. The facial features are detected and analyzed using Haar feature selection like the positioning, distance and the geometric shape of

the eyes, nose, ears and jaw bones and then using the information driven from Haar-Feature selection, an integral image is formed [46].

A sub-window of 24x24 pixels can exhibit a total of 162,336 possible features and it would be time consuming as well as expensive and considered to be quite an impractical approach for the facial recognition [47]. Hence Adaboost trainer is used which eliminates the scanning of all insignificant features and also train the classifiers to recognize the relevant features. Once an integral compressed biometric template of two-dimensional is formed, the features stored in the layout are converted into as set of Eigenvectors and thus an Eigen face is formed. The formation of Eigen face is to speed up the analysis and to reduce the response time as shown in Fig. 6. Facial recognition is implemented through a cascaded classifier of GPCA and KNN algorithms. KNN is a nonparametric formula used in classification of data. It is also used in pattern recognition. It is one of the simplest algorithms of machine learning for pattern recognition [48].

Figure 8.5: Face Detection Using Viola Jones Algorithm with Rectangular Haar Feature Selection

PCA is an algorithm that converts the correlated elements to linearly uncorrelated elements through orthogonal transformation. In Generalized PCA, the condition of orthogonally is removed to consider an arbitrary number of spaces of unknown and different

dimensions [49]. The cascaded classifier uses the comparison of Eigenvectors of the stored bio-metric template with the digital image of the voter generated at the time of voting and then compares the nearest numbers of similarities by introducing a test vector from the live scan of the voter. If the similarities is less than 90% keeping in mind the environmental light and tolerated offset angles, the similarities will be rejected and the voter won't be able to cast his/her vote. Although many methods of face detection are present of which the cascaded classifier method by using local PCA and LDA but their resulting accuracy is quite low as compared to GPCA and KNN. Fig. 7 shows the comparison of the accuracy of GPCA and KNN with LPCA and LDA in the next section of this paper. Apart from that the response time for the cascaded classifier of GPCA and KNN method is quite fast and responsive as compared to the other methods usually employed for face-recognition which will be discussed in the results and discussion section.

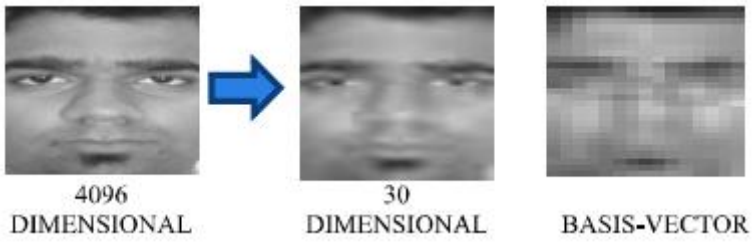


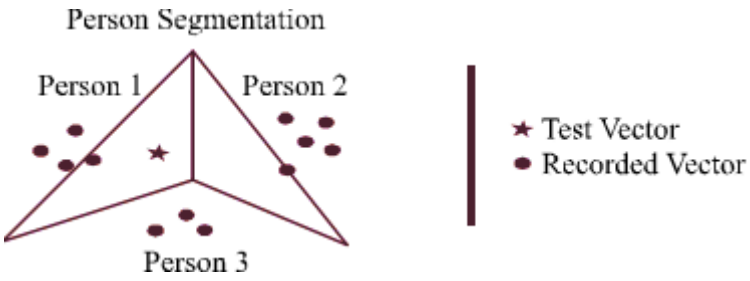
Figure 8.6: Feature Reduction and Formation of Eigen Face

Fingerprint Processing: The method employed by the finger print module is the optical method. Optical finger print verification technique maybe defined as the formation of a biometric template from the digitally computerized image for verification using visible light [30]. The surface for scanning the finger print is called as touch surface and underneath there is a light-transmitting phosphor layer which enlightens the surface of the finger.

The light reflected from the finger goes through the phosphor layer to a variety of strong state pixels which captures a visual picture of the finger print [31]. The algorithm used for the finger print verification is a pattern-based verification in which the digital image of the

finger print is compared with the previously stored bio-metric layout on the basis of similarities of the minutiae features like ridge ending, bifurcation, and short ridge [32].

The figure 8.6 shows the minutiae features of a finger. The pre-stored template containing the features of minutiae features are compared with the finger print of the voter and if the comparison yields less than 90%comparison keeping in mind the tolerated offset angle, then the voter won't be allowed to vote.



Results and Discussion:

In this section, the results of the proposed electronic voting system are presented along with comparison with other systems. The distinct and outstanding features of the proposed system are that the facial recognition algorithm is unique and the accuracy yielded as compared to other cascaded algorithms is high. The table 8.1 shows the result of the experimental outcome of the electronic voting system for different K-Values: The finger print module is also tested and its accuracy is shown in table 8.2. The figure 8.9 shows a comparison between KNN and a cascaded classifier i.e. GPCA and KNN. The results show that the cascaded system gives higher accuracy than individual KNN classifier

Figure 8.9: RIDGE DOT [30]

TABLE 1. FACIAL TESTING OUTCOME

Faces tested	Correct	Incorrect	Missed	Accuracy
100	91	3	6	91%

TABLE 2. FINGER PRINT TESTING OUTCOME

Tested	Correct	Incorrect	Missed	Accuracy
100	98	0	2	98%

The use of cascaded classifier of KNN and GPCA rather than just using KNN and the outcome comparison of their accuracy with respect to changing number of Kvalues compared in a single cycle can be seen in Fig. 9 having an accuracy of 91% for a preset value of k=1 in the implemented system. Also from the results and comparison of outcome of other studies and research papers, the accuracy of the outcome of separate and paired classifiers at a constant dimension is shown in Fig. 10 for comparison of 1764 distinct features and a K-value of 1 (for algorithms using K-NN). the experiment carried out yielded the following results which are interpolated in figure 11 which shows a relation between distinct features in pixelated form stored in a biometric template and its effect on time response and was found to increase with the increasing number of distinct features and founded that the algorithm had a response time of 4.32 seconds for a 1764 distinct features and k-value=1 (k-value is the number of features compared per cycle) as preset in the system for real-time implementation.

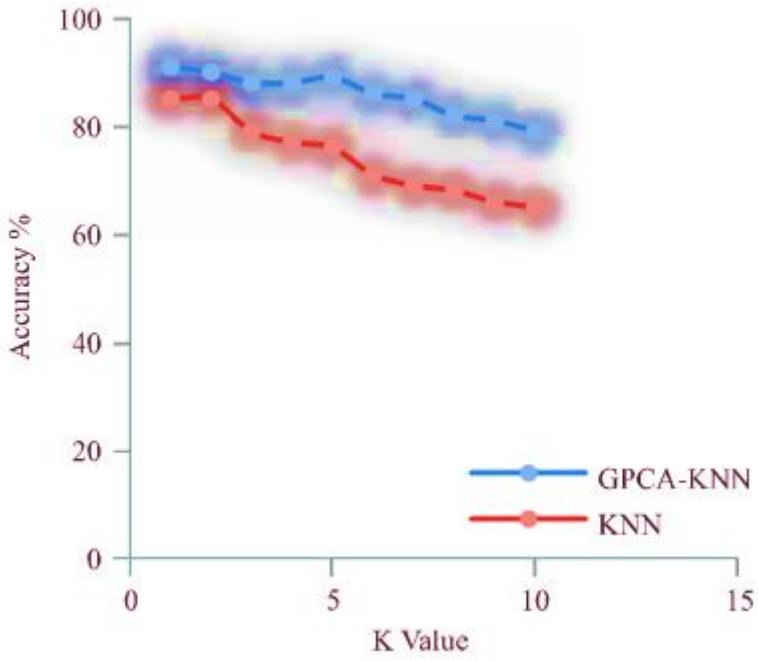


Figure 8.10: Comparison of Accuracy between KNN and GPCA+KNN

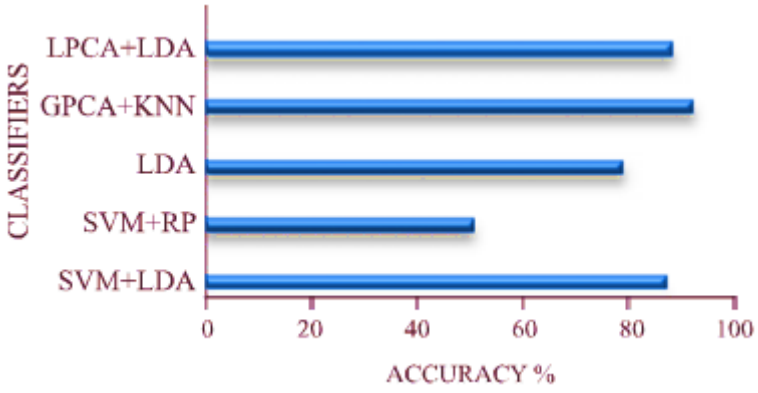


Figure 8.11: Accuracy of Different Classifiers

Figure 8.11 shows the comparison of the accuracy of GPCA and KNN with LPCA and LDA with respect to the distinct features compared with the features stored in the biometric template as preset in the algorithm for testing and having an accuracy of 91% (approximately) and k-value=1 (k value is the number of features compared per cycle) for the 1764 distinct features

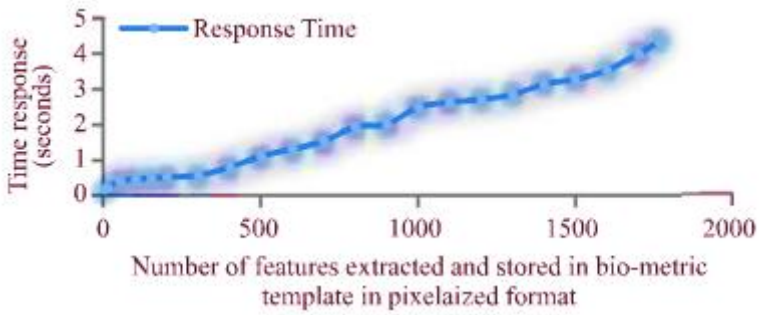


Figure 8.12: Response Time with Varying Dimensions

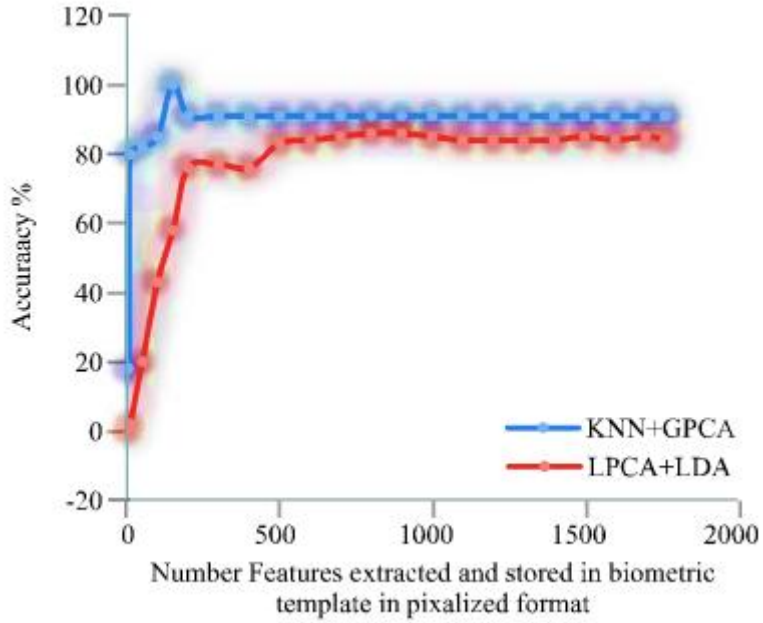


Figure 8.13: Comparison of Accuracy with Different Cascaded Classifiers

CHAPTER IX

CONCLUSION AND RECOMMENDATIONS

The design of e-voting systems for electronic democratic decision making must embody a list of generic security requirements of authentication, confidentiality, integrity and non-repudiation. Without these requirements, rigging, fraud and corruption in electoral process will ultimately mar the integrity of the electoral process. Various attempts in literature had proposed and developed secure e-voting systems using cryptographic models, steganographic models and combination of both to these generic security requirements in piece-meal. This had established gap of developing a concurrent, multi-layer (stegano-cryptographic) and multimedia (Image/video) e-voting model for driving future free, fair and credible e-democratic transition in developing country like Nigeria.

In this workr, an enhanced stegano-cryptographic e-voting model has been developed for an architectural framework of secure e-voting in poll site, web and remote mobile voting scenarios. This was achieved using Software Engineering, Information Hiding techniques and Information Systems Design approaches by careful combination of evolutionary spiral and unified process software process models. A secured e-voting system was modeled and developed on the Stegano-Cryptographic e-voting model for pre-electoral, electoral and post electoral processes where voter's registration, ballot casting and vote audition were accomplished on mobile platforms.

The performance of developed e-voting model was quantitatively evaluated on the secure e-voting system application for fundamental security requirements of evoting. The developed model is 37.58% and 16.14% better than Shamin and kattamanchi (2012) and Kamau et al., (2013) in frequency and Spatial domain respectively. The result of the evaluation shows that the developed e-voting model has an appreciable attribute of secure e-voting system with high degree of authentication, integrity, confidentiality and auditabillity

for the delivery of transparent, free, fair and credible electronic democratic decision making in the developing countries where significant digital divides exist.

The enhanced secure e-voting model was developed to address these fundamental security issues to evoting in developing countries with peculiar and massive access to high end infrastructural ICT facilities. Therefore, it is recommended that government organizations like Independent National Electoral Commission (INEC) in Nigeria should embrace the findings of this research to facilitate credible, transparent, free and fair edemocracy in future elections.

Future research in the field of security in electronic voting should look at the following open issues:

- Security of e-voting system against DoS and DDos Attacks. : Denial of service (DoS) is an attempt to make computing resource unavailable by saturating the target device with external bogus and unnecessary communications request. Future research could provide mechanism to increase and protect the developed secured model for attacks due to DoS and DDoS.
- Voters' Coercibility: Although the developed e-voting model ensures voter's authentication and validation through multifactor authentication, an open issue of debate is how the voting system would prevent voters from selling their vote prior to voting. Future research should look at issue of non-coercion in secure e-voting system.
- Quantification of Communication and Network Resource Requirements: Models for the quantification of communication and network resource requirements like bandwidth, throughput and packet size could also be developed to quantify the communication and network resources requirement for proper functioning of secure e-voting model;

- Exploration of Audio cover and Audio Steganographic Techniques: Future steganographic investigation could also look at audio steganographic technique using audio cover for covert communication security in e-voting systems. With the achievement of above recommendations, government and its election authority could increase public participation, political trust and confidence while solving security problems in e-democratic decision making in future elections.

REFERENCES

1. X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, “Blockchain voting: publicly verifiable online voting protocol without trusted tallying authorities,” Future Generation Computer Systems, vol. 112, pp. 859-874, 2020.
2. M. Chaieb and S. Yousfi, “LOKI vote: a blockchain-based coercion resistant e-voting protocol,” in Information Systems. EMCIS 2020, M. Themistocleous, M. Papadaki, and M. M. Kamal, Eds., vol. 402 of Lecture Notes in Business Information Processing, pp. 151-168, Springer, Cham, 2020.
3. D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, “Decentralized voting platform based on Ethereum blockchain,” in 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), pp. 1-6, IEEE, Beirut, Lebanon, November 2018.
4. K. M. Khan, J. Arshad, and M. M. Khan, “Secure digital voting system based on blockchain technology,” International Journal of Electronic Government Research (IJEGR), vol. 14, no. 1, pp. 53-62, 2018.
5. H. Yi, “Securing e-voting based on blockchain in P2P network,” EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, Article ID 137, 2019.
6. B. Madhuri, M. G. Adarsha, K. R. Pradhyumna and B. M. Prajwal, "Secured Smart Voting System using Aadhar," in Indian Journal of Science and Technology, Print ISSN: 0974-6846, Online ISSN: 0974-5645
7. Prachi Zalte, Sonali Gajare, Vaibhav Gujarathi, S. J. Pawar " Centralized Electronic Voting System”, International Journal of Computer Applications (0975 - 8887) Volume 179 - No.27, March 2018.
8. Maliha Khan, Rani Astya, "Face Detection and Recognition Using Open CV" Vol 9(10). DOI: 10.17485/ijst/2016/v9ilo/88 898, ISSN: 0974-5645, March 2016.

9. M. Rajesh, Priyanka, Yuvraj Singh, Shivaraj, "Online Voting System", DOI: 10.1109 /tencon.2015.7373171, IJRASET, 2015
10. Neha Roy, Nouroza Bagwan, Suryakant Godase, Aishwaraya Shende "Smart Online Voting System through OTP Authentication and Face Recognition," DOI: 10.1109/indicon.2015.7443652.
11. Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). "Star-vote: A secure, transparent, auditable, and reliable voting system.", in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.
12. Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). "A fair and robust voting system." by broadcast, 5th International Conference on E-voting, 2012.
13. Adida, B.; 'Helios (2008). "Web-based open-audit voting", in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335348.
14. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008). "Scantegrity: End-to-end voter-veriable opticalscan voting", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.
15. Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). "Bingo voting: Secure and coercion- free voting using a trusted random number generator.", in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.
16. Adida B. and Rivest, R. L. (2006). "Scratch and vote: Self-contained paper-based cryptographic voting." in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40.

17. Chaum, D., Ryan, P. Y. A. and Schneider, P. Y. A. (2005). "A practical voter-verifiable election scheme", in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 118-139.
18. Chaum, D. (2004). "Secret-ballot receipts: True voter-verifiable elections." IEEE Security Privacy, vol. 2, no. 1, pp. 38-47, Jan 2004.
19. Chaum, D. (1981). "Untraceable electronic mail, return addresses, and digital pseudonym", Commun. ACM, vol. 24, no. 2, pp. 84-90, Feb
20. S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain" ICT Express, vol. 6, no. 2, pp. 93-97, 2020.
21. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: extending bitcoin's proof of work via proof of stake [Extended Abstract]y," ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3, pp. 34-37, 2014.
22. S. King and S. Nadal, "Ppcoin: peer-to-peer crypto-currency with proof-of-stake," vol. 19, no. 1, pp. 1-6, 2012, Self-Published Paper.
23. S. Khan, A. Arshad, G. Mushtaq, A. Khalique, and T. Husein, "Implementation of decentralized blockchain e-voting," EAI Endorsed Transactions on Smart Cities, vol. 4, no. 10, Article ID 164859, 2020.
24. V. Anilkumar, J. A. Joji, A. Afzal, and R. Sheik, "Blockchain simulation and development platforms: survey, issues and challenges," in 2019 International Conference on Intelligent Computing and Control Systems (ICCS), pp. 935-939, IEEE, Madurai, India, 2019, May.
25. W. M. Lee, "Using the Meta Mask crypto-wallet," in Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript, pp. 111-144, Apress, Berkeley, CA, 2023.

26. S. Van Hijfte, “Hyperledger and DAGs,” in Blockchain Platforms, Synthesis Lectures on Computer Science, pp. 191- 207, Springer, Cham, 2020.
27. G. Ayoade, V. Karande, L. Khan, and K. Hamlen, “Decentralized IoT data management using blockchain and trusted execution environment,” in 2018 IEEE International Conference on Information Reuse and Integration (IRI), pp. 15-22, IEEE, Salt Lake City, UT, USA, 2018, July.
28. H. Zhong, Y. Sang, Y. Zhang, and Z. Xi, “Secure multi-party computation on blockchain: an overview,” in Parallel Architectures, Algorithms and Programming. PAAP 2019, H. Shen and Y. Sang, Eds., vol. 1163 of Communications in Computer and Information Science, pp. 452-460, Springer, Singapore, 2020.
29. S. Sah, B. Surendiran, R. Dhanalakshmi, and N. Arulmurugaselvi, “A survey on hyperledger frameworks, tools, and applications,” in Internet of Things, Artificial Intelligence and Blockchain Technology, R. Kumar, Y. Wang, T. Poongodi, and A. L. Imoize, Eds., pp. 25-43, Springer, Cham, 2021.
30. Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & Okediran O.O (2014b),” Performance Evaluation of Modified Stegano-Cryptographic model for Secured E-Voting”, International Journal of Multidisciplinary in Cryptology and Information Security (IJMCIS), Vol. 3 No.1,pp. 1 -8.
31. Olaniyi O.M., O.T Arulogun, E.O. Omidiora, & Okediran O.O (2014c),” Implementing generic security Requirements in e-voting using modified Stegano-cryptographic Approach”, International Journal of Information and Computer Security (IJICS), Inderscience Publishers, In press
32. Prabha, S. M. and Ramamoorthy, S.(2012),” A Novel Data Hiding Technique based Bio-secure Online voting system”, Proceedings of International Conference on

Computing and Control Engineering(ICCCE2012),1- 4, Retrieved online at http://www.iccce.co.in/papers/icccecs143.pdf

33. Prasada, R.G (2012), "Random Number Generation and its better Technique", MEng Disseration, Thapar University, Patiala, India.
34. Quan, L and Hong L (2008)," Application of Digital Watermark and Mobile Agent in Copyright Protection System", Proceedings of IEEE International Conference of Computer Science and Information Technology, Singapore, pp1-4.
35. Rura, L., Isaac, B. and Haldar, M. K., (2011), "Secure Electronic Voting System Based on Image Steganography", Proceedings of IEEE Conference on Open systems (ICOS2011), Malaysia, pp 80-85.
36. Shamin A.L and kattamanchi H (2012)," Secure Data transmission Using Steganography and Encryption Technique", International Journal of Cryptography and Information Security, Vol.2 No 3,161-172.
37. Jesus M (2003)," The Importance of ICT for developing Countries", Interdisciplinary Science Reviews", Vol. 28 No.1 pp 10-14.
38. Wang, Z , E. P. Simoncelli, and. Bovik, A. C, (2003), "Multi-scale Structural Similarity for Image Quality Assessment," In Proceedings of IEEE Conf. Signals, Systems and Computers, vol. 2, pp. 1398-1402.
39. Vncent O.R and Adepoju O. K.. (2013)," On Image quality assessment Using Structural Similarity Index", Proceedings of the 11th International Conference on Electronic Government and National Security, Nigeria Computer Society(NCS),pp 104-109.
40. Kohno T., Stubblefield A., Rubin A. and Wallach D. S, (2004), "Analysis of an Electronic Voting System", In Proceedings of IEEE Symposium on Security and Privacy 2004, pp. 1-23.

41. Abo-Rizka M and Ghounam H.R (2007), "A Novel E-voting in Egypt", International Journal of Computer Science and Network Security", Vol.7, No.11,pp 226-234.
42. Manish K, Suresh K.T, Hanumanthappa. M, Evangelin G.D (2005), "Secure Mobile Based Voting System", Retrieved online at http:// www.iceg.net/2008/books/2/35_324_350.pdf on November 17th 2012.
43. Rossler T.G (2011),"E-voting: A survey and Introduction", Available at http:// wiki.agoraciudadana.org/images/5/56/an%2bintroduction%2to%2belectronic%2bvotng%2bschemes.pdf Retrieved on 15th June 2012.
44. Avi Rubin (2001),"Security Considerations for Remote Electronic Voting over the Internet", AT&T Labs - Research Florham Park, NJ. Available at http://avirubin.com/ evoting.security.html, (date accessed 7th July, 2012).
45. Ciprian Stănică-Ezeanu (2008), "e-Voting Security", Buletinul Universităţii Petrol - Gaze din Ploieşti, Vol. LX (2), pp 93-97
46. Okediran O. O., Omidiora E. O. Olabiyisi S. O., Ganiyu R. A. and Alo O. O. (2011)," A Framework for a Multifaceted Electronic Voting System" , International Journal of Applied Science and Technology Vol. 1(4), pp 135 - 142.
47. Akinmosin D., Egbedokun G.G.O. and Ibitowa F.O (2011),"An Extended Multifactor Authentication in Mobile Financial Transaction Using User Authentication Module with Multilayered Encryption Algorithms", African Journal of Computer and Information Communication Technology, ICT (Journal of IEEE Nigeria Computer Section),V ol. 4 (2), pp 17-24.
48. Olaniyi, O.M, Adewumi D.O, Oluwatosin E.A, Arulogun, O. T and Bashorun M.A (2011), "Framework for Multilingual Mobile EVoting Service Infrastructure for Democratic Governance ", African Journal of Computing and ICT (Journal of IEEE Nigeria Computer Section),Vol 4, (3), pp 23 - 32.

49. Olaniyi, O.M, O.T Arulogun, E.O, Omidiora, A Omotoso, Ogungbemi O.B. (2012), " Design of A Secured Model For Electronic Voting System Using Stegano-Cryptographic Approach ", Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2012), National Defense College Abuja, pp 84-89.
50. Ibrahim S, Kamat M, Salleh M, and Abdul Aziz S (2003), "Secure voting using blind signature". Available at URL http://eprints.utm.my/3262/1/ieee02-evs_full_paper_ver14nov.pdf Retrieved on November17th 2012
51. NSF (2001)," Report on the National Workshop on Internet Voting: Issues and Research Agenda", National Science Foundation, Retrieved at http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.
52. Abdulhamid S M , O.S. Adebayo, D. O, Ugiomoh, M. D Abdul Malik (2013), "The Design and Development of Real Time E-Voting System In Nigeria with Emphasis on Security and Result Veracity ", International Journal of Computer Network and Information Security", Vol. 5, pp 9-18, Retrieved Online at http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-2.pdf on 7th August 2013.

View publication stats