**MOBILE FINGERPRINT VOTING**

**SYSTEM WITH BLOCK CHAIN**

**BY**

# OLATUNJI VICTOR 18/1789

**EWURUM PRINCEWILL OZIOMA 18/1973**

**A PROJECT WORK SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE B.SC(HONS) DEGREE IN SOFTWARE ENGINEERING TO THE SCHOOL OF COMPUTING AND ENGINEERING SCIENCES, BABCOCK UNIVERSITY,**

**ILISHAN-REMO, OGUN STATE**

**SUPERVISOR: Dr AJAYI WUMI**

**October 2021**

**Declaration**

We hereby declare that the project “ONLINE FINGERPRINT VOTING SYSTEM” was carried out by

OLATUNJI VICTOR ABIODUN 18/1789

EWURUM PRINCEWILL OZIOMA 18/1973

**Dedication**

This project is dedicated to the Almighty God, who granted us the wisdom, knowledge, and understanding from the start of this project to the very end. We also dedicate this project to our parents, friends and family members who contributed in no small measure to making our stay at Babcock University a wonderful experience

**Certification**

I certify that this project was carried out by the following students under my supervision in the Department of Software Engineering, Babcock University, Ilishan-Remo, Ogun State, Nigeria.

OLATUNJI VICTOR ABIODUN 18/1789

EWURUM PRINCEWILL OZIOMA 18/1973

**Project Supervisor:**

Dr AJAYI WUMI

**Head of Department:**

Dr. ADEKOLA OLUBUKOLA

**External Examiner:**

# ABSTRACT

A credible election is essential for democracy's survival, and voter confidence is essential for civic order. Electoral infrastructure security, accessibility, verifiability, and transparency are all too often compromised. This paper proposed an election system that is fully automated, unbiased, and online in order to simplify the voting process, increase security, reduce manipulation of votes, and reduce counting time. Due to advances in technology and the rapid expansion of mobile technology, outdated voting techniques can be replaced with sophisticated technology in today's globe. The mobile voting technology makes voting more convenient, simple, and efficient. This ensures a secure and quick voting process.

The project is to be designed with an android based system that splits into sections, the first of which is the voter/candidate registration phase (where the voters will be ask to fill a form and fingerprints to verify if the user is the owner of the device and also password will be generated for non-android users while the candidate will just have to register and upload manifesto), and the second of which is the actual voting phase(login will be via fingerprints and passwords and select a candidate of choice) and the last is the block chain phase ( hashing of votes and it will be saved to the database). During the voter registration process, a database including the voter's unique identity number and fingerprint information will be kept in a repository.

Some attributes that the proposed system satisfies are: anonymity, scalability, speed, accuracy, flexibility, and security and it will a web based and mobile system that facilitates the running of elections and surveys online. This system will be developed to simplify the process of organizing elections and make it convenient for voters to vote once remotely from their any devices while taking into consideration security, anonymity and providing auditioning capabilities. The system can be used in various areas where election will be held. The system provides the online registration form for the users before voting and makes the users to cast their vote online. The system is to be developed with security and user friendliness in mind.

**Keywords:** **Mobile voting system**, **Blockchain**, **Fingerprints, Database, Election**

**TABLE OF CONTENT**

Title Page i

Declaration ii

Dedication iii

Certification iv

Abstract v

**CHAPTER ONE: INTRODUCTION**

1.1 Background of Study

1.2 Statement of The Problem

1.3 Aim and Objectives

1.4 Justification of The Study

1.5 Significance of The Study

1.6 Scope of The Study

1.7 Methodology Overview

1.8 Organization of Other Chapters

**CHAPTER TWO: LITERATURE REVIEW**

2.1 Introduction

2.2 Supporting Theoretical Background

2.3 Review of Closely Existing Related Works

2.4 References

**CHAPTER THREE: METHODOLOGY**

3.1 Introduction

3.2 problem presentation

3.3 conceptual Design

3.4 Method of operation

3.5 Design

3.6 ACTORS AND THEIR USE CASES

3.7 REQUIREMENTS

# 

# CHAPTER ONE

**1.1 Background Statement**

In an anonymous voting scenario, this project proposes development of a mobile voting model based on the usage of block-chain and biometric technologies for voter verification and identification, as well as ballot security.

The system will also allow candidate to register and upload manifesto via the login portal. The admin will verify list of candidates that have registered the election. Only the Admin will have full access to the server in the case of creating an election, modification like to verify or remove nominated candidates and registered voters. The number of candidates added to the system by the admin will be automatically deleted after the completion of the election. Admin has to add the date when the election going to end.

The user(voter/candidate) registers and upload fingerprint, a user id and password will be generated for subsequent logins and vote for the candidate who are nominated. The system will allow the user to vote for only one candidate. The system will allow the user to vote for once for a particular election. The admin can verify any number of candidates when the new election will be announced. The admin can view the election result by using the election id. The users will also have access to view the election results.

**Merits of the Proposed System:**

* The system will not allow the voter to cast his/her vote twice.
* The system will allow the voter to vote for two candidates under the same category.
* The system will exploit the android biometric(fingerprint) system to valid the user through his/her phone .

**Demerits:**

* The system might not recognize the user if the voters finger pattern has some cut or got damaged or is not present
* The system is to won’t allow to voters to use a phone. Every voter would required to use their phone.

1.2 **Problem Statement**

In the most recent election involving the Student Association of Babcock University and Its Computer’s Club, it has been observed that there is primarily a major issue whereby a voter gets to vote more than once. The above factor creates a situation whereby the election is deemed not credible enough, or fair. Thus, there exists a vacuum for a system with features that would curb the inefficiencies of the current system.

It has become all too common for some forces to engage in rigging, which may result in a conclusion that differs from the people's genuine verdict. Today, security is a big issue, and it is also necessary to verify that no one votes twice. The aforementioned problems may be handled to some great extent by implementing the mobile fingerprint voting system with block-chain. This will also prevent bogus votes. It's a program that recognizes the user based on his finger pattern. Because each person's finger pattern is unique, the voter may be easily identified. The technology allows voters to verify their ballots using their fingerprints. Fingerprint is used to uniquely identify the user. Fingerprint is used as an authentication of the voters.

1.3 **Aims and Objectives**

This project aims at designing and implementing a mobile fingerprint voting system with block chain.

The specific objectives of this study are;

* To implement the use of fingerprint as a means of voter authentication, mitigate unauthorized and multiple voting hence promoting transparent voting exercise.
* To improve the integrity of voting with the use of block-chain method hence ensuring votes aren’t altered and improving user’s confidence in the integrity of the voting exercise.
* To bring elections to the user directly and promoting the ease of voting through the mobile platform.
  1. **Justification of The Study**

The study will cut down on the amount of time spent in long lines at polling locations during voting. It will also allow people to vote from anywhere on the planet, as mentioned, because this is an internet-based program. Vote miscounts will also be resolved, since the system's back-end has a well-developed database written in MYSQL that can deliver the right data when queried appropriately. Because the voting process will begin as soon as possible, voters will have plenty of time to determine when and for whom to vote.

The fingerprint voting system with block-chain provides a range of advantages to the voting process. It assists perform voting in much more successful and efficient way, such as minimize human error in voting final result as well as minimize the expenses of the election. The significant advantages of electronic election might be reviewing in the following points: much more participation, fast process, lower costs, and precision placing, better and secured access and voter anonymity.

Essential reason fingerprint readers are widely used is, they offer a fast, simple, powerful, and secure access by means of a person with the good access rights can authenticate. The advocate of electronic voting provides that the comfort, flexibility, speed, cost effectiveness, and versatility and these are the main advantages of the electronic voting machine. Considering that this system has every one of these properties, it can be used almost everywhere, by the government authorities, organizations, courts, shopping malls even in the colleges and universities.

* 1. **Significance of The Study**

This study would help increase the level of trust in the entire Student’s Association electioneering processes and also improve on the existing online voting system used in the most recent Babcock University Student Association and Babcock University Computer Club’s elections thus making it more accurate, transparent, secure and faster and will ensure a single vote for a single person, ultimately leading to the conduct of a more credible elections.

Over the years technology related systems were being developed to resolve some of the issues like electoral fraud, impersonation, double voting etc. There are still a few very important areas which have to be identified and addressed, the security which involves a person be able to vote in a secure manner, the time spent for voting by voters, the efficiency in counting of votes and the cost involved in employing people towards monitoring the voting process. So, taking these areas/issues into consideration we have now come with the fingerprint authenticated mobile voting system.

During the registration and voting processes, fingerprint identification will be used. To improve the security of the voting system, passwords will be generated as a form of authentication before registration and after the voter begins the voting process for non-android users or eligible voters whose finger pattern has been severed or destroyed.

* 1. **Scope of The Study**

The scope of this project revolves around the developing of an online voting system that employs fingerprint registration which will allow voters to participate in the elections regardless of their physical location. BUSA and BUCC Elections in the University has been adopted as the case study for the system to be developed

* 1. **Methodology Overview**

The methodology of choice is Rapid Application Development (RAD); this is because the objectives of RAD include high speed, high quality and lowered cost. RAD emphasizes the use of special techniques and computer tools to speed up analysis, design and implementation phases. Tools include Computer Assisted Software Engineering (CASE) tools (such as Requirement Analysis, Structure

Analysis, Software Design, Code Generation, Test Case Generation and Reverse Engineering Tool), Joint Application Design (JAD) and fourth generation programming languages (mainly in database programming and scripting. Examples are Python, SQL). All of which are inline and essential to the proposed system.

The RAD methodology goes through the following phases:

**1.4.1 Requirements Planning Phase**:

It refers to a review of the areas immediately associated with the proposed system. Areas associated with the proposed system include:

1. **Mode of User Voting**: The proposed system would schedule elections by going through the following:

* Voters access the online voting portal and logs on with their personal voter’s Identification Number, in order to view to the voting page.
* On submission of the login request, the system checks to see if the specific voter is eligible to vote in the particular election and performs appropriate actions based on the result status returned from the check.
* If anyone is ineligible to vote, the system displays a corresponding message to the voter that he/she is not permitted to vote.

**2.** **Mode of Voter Authentication**: This achieves our objective of ensuring a secured method of validating voters before they are allowed to cast their votes. Voters would be authenticated by verifying the unique identity details possessed by them. A common and easily implemented mode of verification is by checking for matching fingerprint

**3. Mode of Data Collection and Verification**: Before voters can be verified, there’s a need for prerecorded data in the memory i.e. database of the system. Consequently, the data of every prospective voter needs to be collected to allow verification.

**4. Mode of Data Communication**: The proposed system would operate on an internet. This allows all voters to have access regardless of location as well as increase their ability to use a range of devices to cast their votes. This is a network only accessible by members of a particular organization.

**1.4.2User Design Phase:**

This stage would use various software modelling tools to illustrate the system’s data and processes and to build a visual representation of critical system components. Also, the programming tools chosen to implement the proposed system were stated. A key milestone of this proposed system is to make it a much user friendly and easy to use.

**1.4.3 Block Chain Network**

Multi-chain environment is selected as the development platform. That's because, whereas Bitcoin's sole purpose is to authenticate monetary transactions, the Multi chain platform allows for a wider range of applications thanks to permission-based access. Because all multi-chain blocks are hashed and saved, no manipulation of multi-chain transaction information is feasible. Multi-chain uses user-based networks to process thousands of financial transactions per second. Multi-chain is currently being used by corporations to benefit from different technologies that were initially designed for use with bitcoin. Block chain technology is linked to Multi-chain.

Block chain technology is linked to Multi-chain. Multi-chain is a new piece of software that allows you to create your own Block-chain strategy. Multichain is a software resource for legal contracts and web-based assets that was created for usage on the bitcoin block chain. For voter authentication, fingerprint recognition is used.

Blockchain, as a collection of linked technologies, is open source, distributed, irreversible, and irrefutable. The entire data is shared to all network members in a public asset ledger. Considered to be the notion of blockchain is the "fifth evolution" of computers and the missing trust layer for the Internet. Satoshi Nakamoto initially revealed it in 2008 as the foundation around which the Bitcoin system was created.

based on (Nakamoto, 2009). The encryption protocol, digital signature, and hashing algorithm were all developed in-house existence.

* 1. **Organization of Other Chapters**

Chapter One of this Project focuses on the introduction for this project, It also focuses on its Significance, Aims and Objectives, Brief Methodology, among other things. Chapter Two give an extensive Literature Review on the project. Within this chapter a table will provides summarizing the works of other researchers as well as gaps found in their works. Chapter three focuses on giving a detailed insight on the methods intended to solve the objectives.

**CHAPTER 2**

**LITERATURE REVIEW**

**2.1 Introduction**

**Elections (Definition, Types and History)**

An election is a formal decision-making process by which a population or society chooses an individual to hold a political office. Elections have been the usual mechanism by which modern representative democracy operates that predates to as early as the 17th Century.

Elections are conducted both by public entities such as the government as well as private and business organizations, for example, choosing representatives for the Board of Directors of a company, professional club leadership and even, used in voluntary associations.

**Types of Election**

In most democratic political systems, there are several types or categories of elections that are held which corresponds to the different layers of public governance or geographical jurisdiction. Common types of election categories thus include

* Presidential Elections
* Parliamentary Elections
* Governorship Elections
* Local Government Elections

Considering our given domain, that is, within the university political sphere, there are also various types of elections that are conducted based on several criteria like Student Union, to mention a little.

The various ethnic groups in Nigeria also have different methods of electing their rulers (e.g. Obas, Emirs, Igwes, etc.) and/or key office holders in their traditional kingdoms.

**Voting Systems**

There are two (2) categories under which voting systems can be classified, namely:

* Traditional or Paper – Ballot Voting Systems
* Electronic Voting Systems

**Paper-Ballot Voting Systems**

The paper-based voting system can be described as the traditional means of voting that has been in used over the ages. It is also the default method of conducting elections in Nigeria as well as other countries around the world. It operates by issuing paper ballots to eligible voters who present themselves at the polling unit on the day of the election. The voter is authenticated by searching for and ticking his or her name on the voters register for that particular polling unit. Indelible ink is used to mark an authenticated voter by dropping the ink on the voter’s left thumb fingernail.

The voter is then expected to proceed to a secret booth to vote a candidate by pressing his right thumb into an ink stamp and placing the inked fingerprint in front of the chosen candidate on the ballot paper given and subsequently required to drop the ballot paper into a ballot box placed in an open place within the polling unit.



*Image of a traditional means of voting by paper*

After the close of polls or voting for the election, the election ballot box for the polling unit is opened by the polling officer, the ballots are counted by the various election judges such as election agents and election officials and the total vote results are reported and entered onto the election results sheet which is also required to be signed by all election judges as well as observers present thus giving authenticity to the declared results.

**Challenges of Paper-based Voting Systems**

The use of paper ballot comes with its own set of challenges as enumerated below:

**Low Reliability**: It is easily breached at times due to the multiple avenues that exists for the voters to make error. Paper ballots constitute a single point of failure if lost or damaged, as ballots or choices cannot be copied without loss of fidelity. It also depends a lot of human judgment to ascertain “Voter intent” and not neglecting the fact that paper is essentially an analogue medium.

**Poor Security**: It can be seen that no checksum or encryption is possible as data must be presented in clear text. Paper ballot can thus be manipulated by hand even by the least of technical personnel and cases of Ballot Box stuffing during and after elections are often rampant. Voters are often at the mercy of political thugs and security personnel.

**High Costs**: There are often high cost incurred during the printing of various election materials, purchase of paper-handling equipment as well as the cost needed to store and transport the materials.

**Voter Intimidation**: There has been cases of harassment of voters during elections, voter coercion and issues of ballot counting discrepancies

**Queueing**: In cases of high voter turnout, there is usually a high probability that queues would be formed by voters often subject to the unpredictable weather conditions such as rains or scorching sun.

Voting provides a means by which members of a society or group are able to choose their leaders. Technology and politics are forming a great synergy that have birthed electronic voting. There two types of electronic voting – poll site voting, where voters must be physically present at designated polling units using the Voting Machine and Remote voting which does not have the requirement of the former.

Biometrics simply means correctly determining the identity of individual features that are unique to that individual. Those features are physiological or behavioral but we’ll focus on the former (fingerprints precisely) for the sake of this project. Physiological features are those attributed to the composition or shape of the human body, such as ear, eye, hand and fingerprints. Fingerprint recognition is focused as a means of identity determination. For fingerprint biometrics, templates (fingerprint images showing bifurcations and ridge endings) are captured and stored in database during voter registration. Identity verification is through comparison of the current image with that of stored template. The bifurcations and ridge endings, collectively known as minutiae are the features through which each individual’s fingerprints are distinguished.

Blockchain, sometimes referred to as Distributed Ledger Technology (DLT), makes the history of any digital asset unalterable and transparent through the use of decentralization and cryptographic hashing. For example, creating and sharing a Google Doc with a group of people, the document is distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the document at the same time. No one is locked out awaiting changes from another party, while all modifications to the doc are being recorded in real-time, making changes completely transparent. Blockchain helps to reduce risk, stamps out fraud and brings transparency in a scalable way for large and countess uses.

The framework (which involves registration, verification, authentication of users) will allow us to evaluate as well as compare the merits of existing and future candidate online voting schemes. Fingerprint recognition technology will provide more security in authentication by providing a unique identity to all users hence maintaining the fingerprints of all the registered users in a database.

The aforementioned frameworks help to streamline efforts and identify necessary properties that a secure and trusted online voting system must satisfy to mitigate double, illegal voting, voting manipulations and other setbacks in voting exercise.

**2.2 Supporting Theoretical Background**

Blockchain is an emerging technology with strong cryptographic foundations, allowing applications to take advantage of these capabilities to build secure solutions. A Blockchain resembles a data structure that stores and shares all of the transactions that have occurred since its inception. It's basically a distributed decentralized database that keeps track of a continually expanding and evolving list of data records that are protected from illegal manipulation, tampering, and change.

Blockchain allows any user to join the network, submit new transactions, validate existing transactions, and build new blocks (Rosenfeld, 2017; Kadam et al, 2015; Nakamoto, 2009). Each block is given a cryptographic hash (which can be thought of as a block's fingerprint) that is valid as long as the data in the block isn't changed. If there are any changes to the block, the cryptographic hash will change quickly, indicating that the data has changed, which might be due to malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across a variety of fields (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015).

Although Bitcoin is the most well-known blockchain application, academics are eager to investigate how blockchain technology may be used to assist applications in a variety of disciplines, utilizing characteristics such as non-repudiation, integrity, and anonymity. In this paper, we look at how blockchain might help with e-voting applications by ensuring voter anonymity, vote integrity, and end-to-end verification. We believe that core blockchain properties like self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records can be used for e-voting. Due to its fundamental nature of maintaining anonymity and maintaining a decentralized and publicly distributed ledger of transactions across all nodes, blockchain technology can play a crucial role in the sphere of electronic voting. As a result, blockchain technology is highly effective at dealing with the risk of using a voting token multiple times and attempts to sway the outcome's transparency.

Our investigation will focus on crucial problems such as voter anonymity, vote confidentiality, and end-to-end verification. These difficulties are the bedrock of an effective voting system that maintains the integrity of the electoral process. We offer our attempts to investigate the usage of blockchain technology to find solutions to these problems in this article. Our method, in particular, is built on the Prêt à Voter strategy (Ryan, 2008) and employs the open source Multichain (Multichain, 2017) blockchain platform as the underlying technology. The system creates a strong cryptographic hash for each vote transaction based on information particular to a voter in order to safeguard the anonymity and integrity of a vote. To enable verification, this hash is also sent to the voter through encrypted channels. As a result, the system meets the essential requirements of an e-voting system as defined by (Rura et al, 2016).

**2.3 REVIEW OF EXISTING WORKS**

**A. Piratheepan, et. al (2017), proposed a Fingerprint Voting System designed using Arduino system.** Its goal is to use voters' fingerprints at the polling booth as proof of identity or to verify if a matching fingerprint exists among those saved in the database prior to authentication. Fingerprint enrolment, finger verification, cast the votes, alert for incorrect voting, and Generate final report are the five modules that makes up the system.

This project, which is quite similar to Electronic Voting System, was created with Arduino (EMV). The device or system reads the data from the Fingerprint module, compares it to previously recorded data, and then proceeds to the next step. The entire system is made up of Arduino, a fingerprint module, and push buttons. The Arduino is controlled by a program written in C/C++ that allows it to communicate with the Fingerprint Module. The Arduino controller compares the data to what it already has in its memory and then executes the orders specified by the controller section.

The work eliminates almost all of the problems associated with the use of paper ballots and also mitigates dual votes from a voter and illegal votes; however, the ease of voting is not promoted because voters cannot make their choices in the privacy of their own homes; voters must still queue at polling sites and wait before casting their votes. Voting can be hacked, and the voting system stolen for illegal voting or vote tampering, making the entire voting process opaque.

**International Journal on Informatics Visualization (JOIV) published a research work (2020) titled “A Proposed Framework for Fingerprint-based Voting System in Bangladesh”, authored by Nahida Nigar, et al.** This paper discusses how Electronic Voting Machines will facilitate voting in one of the world's most populous democracies. Conducting free and fair elections in nearly every populous country is a difficult undertaking for the electoral commission.

The goal of this project is to enhance the current voting system in Bangladesh such that it is more accurate, transparent, and speedier, and that each person has only one vote. Every human being's thumb impression has a unique pattern, the system uses it for voter identification so as to ensure only authorized/registered voters have access to voting rights. As part of the pre-poll procedure, a database of all eligible voters' thumb impressions in a constituency is created.

While it simplifies efforts to eliminate repeated votes from a voter and illegal ballots, the convenience of voting isn't promoted because voters can't make their choices in the privacy of their own homes; instead, people must queue at polling stations and wait before casting their votes. Voting can be hacked, and the voting system stolen for illegal voting or vote tampering, making the entire voting process opaque.

**B. U Umar, O. M Olaniyi, et al., proposed for a Development of Fingerprint Biometric Authentication System for Secure Electronic Voting Machines (2019).** This work concepts the inclusion of biometrics as a means of voter registration, verification and authentication in the development of electronic voting system to meet certain requirements (Transparency, Auditability, Uniqueness, Simplicity and Integrity) of a secure voting system.

The hardware components of the system comprise of Raspberry Pi 3B+, ZFM-60 fingerprint sensor, 7” touchscreen display. The software components are the web GUI and the fingerprint registration and authentication element. The software development was concerned with the Raspberry Pi control program that controlled inputs from the input unit, controlled the flow of data within the control unit, as well as the elements to be displayed on the output unit. The Raspberry Pi software features code that initialized all the output and input units, collected and compared data from the fingerprint module using Python scripts and used matching algorithms to compare the data, used HTML, CSS and JavaScript for the display to render info to the user in a simple User Interface through the touchscreen. PHP and MySQL are used for communication between the web interface and the database tables that hold voter and voting data.

This project presented a powerful electronic voting machine that adequately resolves the challenges of authentication, transparency, high accuracy and credibility in voting systems. The system used touchscreen interface for easy user interaction with the system. Therefore, the combination of the fingerprint biometric authentication and secure voting enables the system to provide a means of holding credible, free and fair elections but it still doesn’t promote the ease of voting neither does it eliminates the queues of waiting voters and voting can be disrupted by hijacking of the systems, leading to loss of votes or even illegal voting.

**International Journal of Applied Engineering Research published a worked titled “IOT BASED VOTING MACHINE WITH FINGERPRINT VERIFICATION” (2020) authored by SHILPA C VENUGOPAL, RESMI K. RAJAN.** The proposed digitize system is based on ThingSpeak (an open-source Internet of Things (IoT) application and API to store and retrieve data from things using the HTTP protocol over the web or via Local Area Network), to be implemented comprises of two units; one for verification and other for voting. In the verification unit there are three scenarios- voting for first time, voting more than once, mismatch in fingerprint and Aadhar number (easily verifiable 12digit random number as Unique Identity issued to all India citizen, whose age is 18 and above).If a user attempts to vote for the first time, his fingerprint and Aadhar number is compared with data in the database, if a match occurs, he can cast vote and message “Authenticated. Proceed” displays on the serial monitor of the Arduino.If an authenticated user tries to cast vote more than once then a buzzer sound will be produced and “already voted” message displays on serial monitor. If the fingerprint and Aadhar number of a person is not available in the database, he can’t cast his vote. In the voting unit, the voter can cast vote by using keypad through the IoT and finally the authorized officer gets the summary of voting.

This system doesn’t promote the ease of voting but it requires less time in getting result, votes aren’t that secure and it can be manipulated.

**Vijay Jumb, Jason Martin, Phyllis Figer, Aniket Rebello proposed Mobile Voting Using Finger Print Authentication (2015).** This project reviews existing voting process or approach in India, then implements an automated online voting system which validates the voters to ensures only legible and registered voters are allowed to vote. The voting platform displays all registered voters’ access rights and privileges in the database to the admin, possesses a friendly user interface and robust enough to resist been corrupt in the event of voting and votes counting.

Voters information are securely stored and retrieved from the database, enabling secure voter login, which means that nonlegitimate voters, such as minors and non-nationals, should never be allowed to use the tool. It also increases the number of voters since it will be easier and more convenient for people to vote from anywhere over the internet at a set time, eliminating the need for people to queue at polling stations before casting their votes.

The system operations like edit, delete, and view, enhances manipulating of records in database hence leading to possible election rigging or manipulation.

**Haydar Imad Mohammed proposed a Fingerprint Base Electronic Voting System project for the degree of BEng (Hons) in Telecommunication Engineering in Asian Pacific University of Technology and Innovation (2013).** The fingerprint model voting system is based of MATLAB program containing registration mode and voting mode where the registration mode is used to register eligible voters, whereas the voting mode is used to allow voters to vote.

The project uses fingerprint technology to for personality proof, reads the fingerprint’s data and compares it with the data previously stored inside the database. If the data in the database matches the previously saved data, the voting system will allow the voter to log in and cast his or her vote. If the data from the Finger does not match the stored data, the system will immediately display a warning and authorities will be summoned to take action. Matching algorithm is designed in an efficient way in order to boost the system’s accuracy.

Uploading a big number of fingerprint images (8bit per pixel for each) to the database necessitates a large amount of memory space, and a large number of voters necessitates additional fingerprint images being uploaded to the database, slowing the database response and resulting in a delayed voting process.

Voting can be disrupted; voting machines hijacked which may even lead to illegal voting and rigging of election.

**ONLINE VOTING SYSTEM USING FINGERPRINT SCANNER authored by Umesh A. Wakpanjar et al. (2018).** The proposed system supports multi-user environment and full automation. This study establishes a framework and identify necessary qualities that a secure and trusted online voting system must satisfy in order to avoid discovery redundancy. We will be able to analyze and compare the benefits of existing and future candidate online voting schemes using such a framework.

The user scans his or her finger on the fingerprint module during the online voting process. If the information or data is stored in a database, the system will verify if the information is correct or incorrect. If the information is incorrect, the user is not eligible to vote; however, if the information is correct, the user is eligible to vote. The web interface's usability determines the system's efficiency and observing voting may be more complicated/difficult to organize. This will undoubtedly assure a more secure voting system, which is essential for a developing country's healthy development.

Remote voting solutions that take place in an unregulated environment may increase the possibility of fraud, coercion, family voting, impersonation, ballot confidentiality violations, and other issues additional tampering with the vote's integrity

**International Research Journal of Engineering and Technology (IRJET) published a work titled: Securing Voting System using Blockchain and Fingerprint Verification, authored by Miss. Komal Kundan Sharma et al. (2019).** The goal of this project is to use block chain technology for transactional purposes. Block chain is a difficult-to-forge digital ledger of economic activities that may be configured to record financial and other transactions. The information saved in block chain is anonymous since it is not linked to personally identifying information. Transparent transactions and verification are possible with block chain. Strong, robustness, anonymity, and transparency are all properties of block chain technology that are beneficial in voting systems.

This is advantageous for a secure voting system. The notion of blockchain, as well as the security approach it employs, immutable hash chains, has become more adaptable to polls and elections as a consequence of our suggested solution.

The adoption of blockchain technology eliminates the chance of election results being tampered with, but a group with greater computer power than the rest of the network can change or generate false blocks. Assailants might include hackers, user groups, and even the Central Election Commission. Another issue is the growth of processing power required to sustain such an infrastructure for the implementation of blockchain technology in elections in the world's most populous country.

**International Journal of Advanced Research (IJAR) published a research Article titled: Secure Online Voting authored by Manjusha Vijay Amritkar, et al. (2016)**. The research proposed an authentication technique for online voting that uses an Eigen Face Detection and Recognition system and finger print impression scanning to achieve the following rules: Only eligible people can vote, no one can vote more than once, the vote is secret, and each (correctly cast) vote is counted. This study will help to boost voting turnout, reduce election expenses, and enhance the accuracy of outcomes. It may employ pulse rate detection to improve user security and prevent blackmail and bullying. It can aid in the reduction of manual processes. It has the potential to decrease human mistakes in vote counting. It has the potential to minimize the amount of manpower necessary in voting booths. It can assist in reducing the amount of time spent. It has the potential to aid in resource conservation. It is capable of ensuring secure vote transfer.

Observing voting may be more complicated/difficult to organize hence it brings voting to the people hence, it might take place in an unregulated environment may increase the possibility of fraud, coercion, family voting, impersonation, ballot confidentiality violations, and other issues. additional tampering with the vote's integrity.

**2.4 References**

M. M. Sarker and M. N. Islam, “Management of sustainable, credible and integrated electronic voting (e-voting) system for bangladesh,” Management of Sustainable Development, vol. 5, no. 1, pp. 15–21, 2013.

Sarker, M. Mesbahuddin, et al. "An approach of automated electronic voting management system for bangladesh using biometric fingerprint." International Journal of Advanced Engineering Research and Science 3.11 (2016).

Iswarya, Deepika, Rathna Prabha, and Trini Xavier. "A Survey on EVoting System Using Arduino Software." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) 5.2 (2016): 687-690.

KARTHEEK, THAMPULA, and B. NAVEEN KUMAR. "Biometric Based Secured Electronic Voting Machine." (2016).

Baig, Hidayat, Taslim, B. Jeba, Rajesh, A. Prof., J., and Prof., “Secured Evoting via smart phone app,” International Journal on Future

Revolution in Computer Science Communication Engineering (IJFRSCE), vol. 2, pp. 20–23, 2016.

M. Yinyeh and K. Gbolagade, “Overview of biometric electronic voting system in ghana,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 7, 2013.

O. M. Olaniyi, Taliha, F. A., Abdullahi, I. M., & Abdusalam, A. K. , “ Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique.,” Journal of Computer Engineering, Vol. 17, No. 6, Pp. 2278 - 2661, 2015.

[10] O. M. Olaniyi, Taliha, F. A., Ahmed, A., & Joseph, O. , “Design of Secure Electronic Voting System Using Fingerprint Biometrics and CryptoWatermarking Approach,” International Journal of Information Engineering and Electronic Business, Vol. 8, No. 5, Pp. 9 - 17, 2016.

[11] H. Srivastava., “A Comparison Based Study on Biometrics for Human Recognition.,” IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 15, No. 1, Pp. 22 - 29, 2013.

**CHAPTER 3**

**METHODOLOGY**

**3.1 Introduction**

In the chapter, the process for the whole development will be discussed.

**3.2 Problems Presentation**

The main problem this system is to address is the security of votes and the fact that election isn’t totally free and fair but can be easily manipulated

**3.3 Conceptual Design**

The project is a mobile based software which will be in constant communication with a database. It will consist of both the front-end which will be done with the use of android studio (XML) and the back-end will be handled with Kotlin. The back-end’s purpose is to connect and communicate with the database. This software is meant to allow the basic user to communicate with the database where they are limited getting information and voting, while candidates will have slightly little more access which will allow them to edit their candidacy information and manifesto get information on the election. The Admins would have full access to the database and can modify it much as possible via the app. The app will be divided into two one version for the Admins and the second for the Candidates and the voters.

**3.4 Method of operation**

This aspect is mainly going to focus on how the software is going to operate the steps and procedures is going to take.

*Block Diagram of the proposed System*

Open App

Register

Upload Fingerprint

No

Match fingerprint?

Candidate selected

Vote Success

Stop

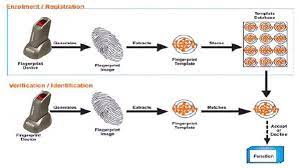
*Flowchart of the Mobile Fingerprint Voting System with Blockchain*

**Voters polling**

This is going to address how the voters are going to register get validated, how their data is going to be protected and their information is not going to be leaked.

**Voters registration and Verification**:

This is the process of getting voters details, verifying and authenticating if it matches the ones uploaded to the database by the admin, the method of execution is going to be by the admins providing a list of expected voters and then the users can generate their unique voter id’s with password with the help of the system, and have access to login and select their votes at the time for the election to take place.



*Fingerprints Enrollment and Verification Process. (Alaguvel R., et al, 2013*)

**Voting process**

With the use of block-chain technology the voters cast their votes via the app to the server which will then in turn hash the information and adds it to the existing hashes in the database, and then sends the total sum of ashes back to the user with a time stamp attached. This will help the system to retrieve back the original hashes when one is tampered with to ensure the integrity of the app

**Candidates polling**

Unlike the method use for voters polling the candidates are going to upload their information to the database for verification and for the voter to access information on who they want to vote

**Candidate registration**:

The candidates would be required to drop their biodata like name, mail, sex, profile picture, etc. Which will be later verified before being cleared to run in the election.

**Candidates verification:**

This is going to be done by putting the uploaded data from the candidates in a temporary location for to either verify or decline which would determine if the data stays on the database or gets deleted.

**Manifesto upload & verification:**

To allow voters to know the agendas of the candidates, the candidate would be provided means of uploading their manifestos which will be verified and the voters would be allowed to view and comment.

**Admins**

They are the ones to have the privilege to create and edit elections via the server and verify anything the candidates uploads. They also have the responsibility of uploading the list of voters to the database which the system will turn use to confirm any voter registering as a valid voter.

**3.5 Design**

The process of the development for this system is broken into three tiers which is mainly the server, mobile app, and the database.

**The Server**:

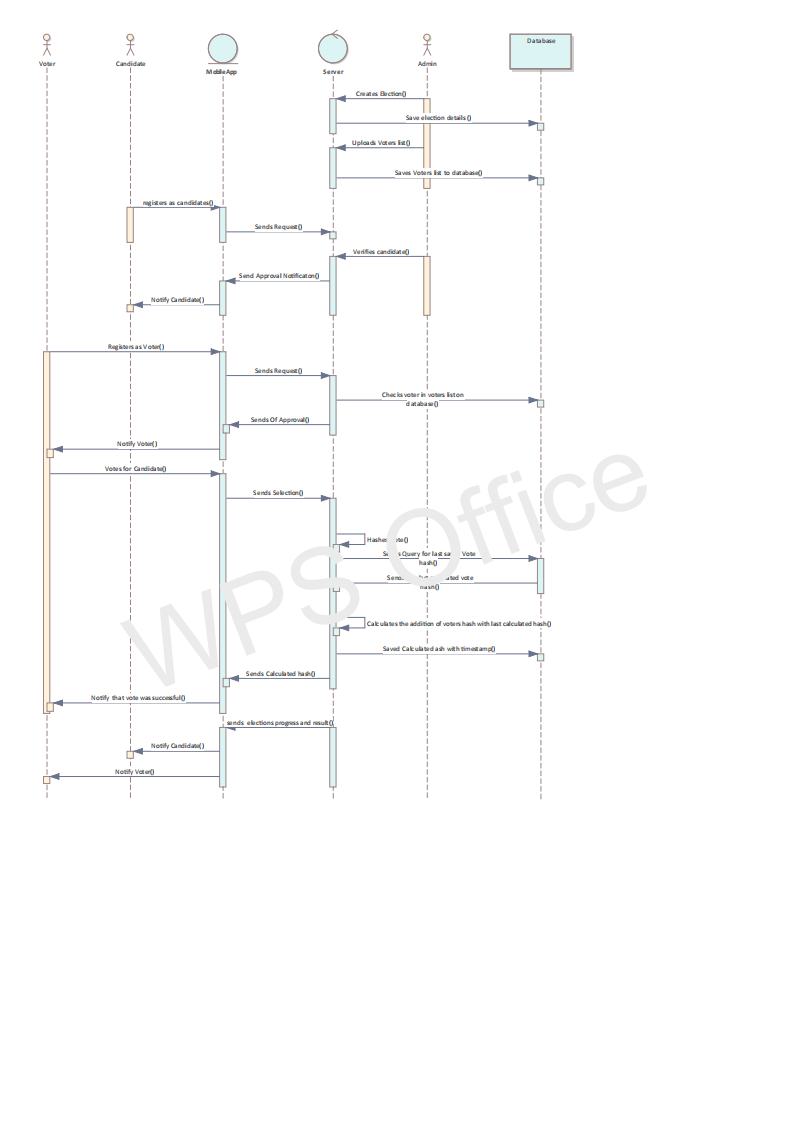
According to Oxford Dictionary “a computer or computer program which manages access to a centralized resource or service in a network.” The servers job in this case is to manage the access of the voters and candidates to the database in the case of the voter it job is to help confirm if the voter intending to register is part of the uploaded voter list and adds their details to the database, in case of the candidate it help saves the data of the candidates in a temporary table and after verifies the data moves it to a table it will be permanently saved the same method applies to the manifestos. The server is going to act like a web site in which the admins can use to have full control of their elections. The server is also responsible for hashing and calculation of the total hashes during the election. And it is also responsible for sending the back to the voters the compile hashes for their elections and the total election.

**The Mobile App**

The mobile app is the part of the system that the voters and candidates use in elections which for the voters allows them to register, make votes, view results, and retrieve computed hashes. For the candidates it allows them to register for election as candidates, upload their manifestos and view election results.

**The Database**

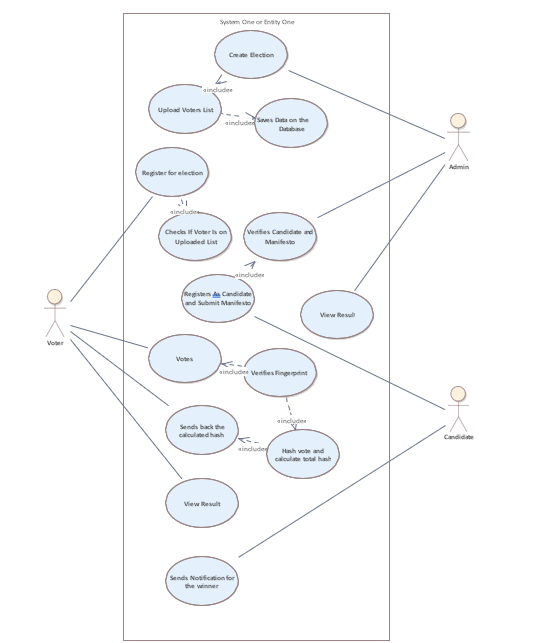
The basic function of this data base is to store information of the election proceedings, voter details, candidates details and manifestos, admins details and system logs.



Sequence Diagram

**Use Case Diagram**

The Use case diagram is a graphic that is used to define the core elements and processes that make up a system. The key elements are termed as "actors" and the processes are called "use cases." It shows which actors interact with each use case.

 *Overall Use-Cases Diagram for the Mobile Fingerprint Voting System with*

*Block-chain*

**3.6 ACTORS AND THEIR USE CASES**

**ACTOR: VOTER**

**USE CASES**:

1**. Register for Election**: This is a major functional requirement of the system. Here the voter’s details as well as fingerprint template is enrolled for validation

This is a functional requirement of the system. It entails the capturing of the voter’s fingerprint image for verification and cross-referencing with the details already uploaded on the database by the Admin. It does a comparison of the fingerprint templates, detecting the minutiae points and matching them.

2. **Cast** **Votes**: The voter is able to exercise their franchise and choose their preferred

candidate for any ballot or post in an election

3. **Receives Hashed Votes**: The voter receives total number of votes hashed as at the time he/she voted.

4. **View Result**: The voter can view the results of all elections that have been closed and stopped

**ACTOR: CANDIDATES**

**USE CASES:**

1. **Register for Election**: This is a major functional requirement of the system. The candidates enroll for the various voters available.

2. **Notification of Winner**: The sends notification of winners to the candidates

**ACTOR: ADMIN**

The ADMIN manages the operation of the Voting module of the Mobile Fingerprint Voting System.

**USE CASES:**

1. **Create Elections**: This is a major functional requirement of the system. The

election officer is required to create new election as well as manage their lifecycle. A

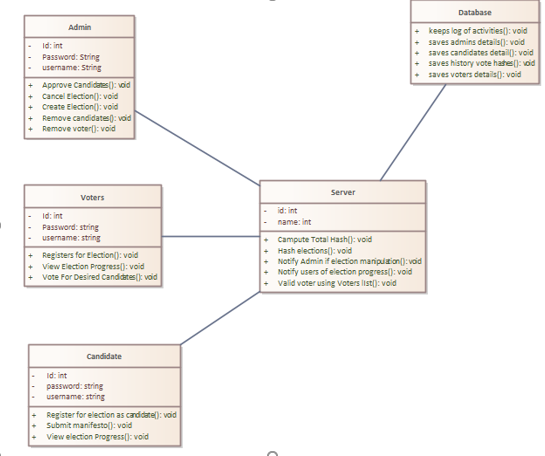
direct sub – function of creating elections on the system is the operation to create ballots or offices or posts for which candidates would be able to contest for.

2. **Verify/Authenticate Candidates and Manifesto**: This allows the election officer to validate candidates for any forthcoming election which has been registered on the online voting module.

.

3. **View Results**: This involve viewing and printing of the completed election results which can also be saved as a pdf file.

**Class Diagram**



*Class Diagram for Mobile fingerprint Voting System with Blockchain*

**3.7 Tools**

The tools to be used for the development of this project are as follows:

* **Rapid Application Development Model:**

Rapid Application Development (RAD) is an agile software development process that emphasizes prototype releases and revisions as quickly as possible. RAD, unlike the Waterfall method, prioritizes the usage of software and user feedback over meticulous planning and requirements documentation.

**Advantages of RAD:**

* Developers may make changes rapidly during the development.
* Code reuse is encouraged, which implies less manual coding, fewer mistakes, and faster testing.
* Increased customer satisfaction as a result of high-level stakeholder engagement and coordination (developers, clients, and end users).
* Better risk management since stakeholders may talk about and fix code flaws while still working on new features.

**Steps in RAD**:

* Define and finalize the project's
* Requirements
* Start making prototypes.
* Obtain customer input and do a test
* Demonstrate your system
* Django
* Kotlin
* MySQL database

**3.8 REQUIREMENTS**

**Hardware Requirements**

* A web server
* An android phone with a fingerprint sensor and a minimum Api level of 27

**Software Requirements**

The software requirements of the application are as follows:

* Ubuntu 20.04
* My SQL Workbench
* MySQL Database
* Android Studio and Kotlin
* Django

**Functional Requirement**s

* Secure storage and retrieval of voters’ details from the database.
* Enable secure login of voters, that is to say non-legitimate voters should never be allowed to login to the tool.
* Maintaining and manipulating records in database through functions like edit,

delete, and view shall be only accessed by the admin only.

* The system must provide the voters with accurate data
* The system must supply standard reports for decision making
* The system must provide standard error checking
* The system must provide data integrity checks to ensure data remains consistent and updated.

**Non-Functional Requirements**

* Mobility: The voter should not be restricted to cast his/her vote at a single place.
* Convenience: The system shall allow the voters to cast their votes quickly, in one session, and should not require many special skills.
* User-Interface: The system shall provide an easy-to-use user-interface.
* Accuracy: The system shall record and count all the votes and shall do so correctly.
* Eligibility: Only authorized voters, who are registered, should be able to vote.
* Uniqueness: No voter should be able to vote more than once for either for a particular candidate or more than one. The voter may also receive a warning of not voting in the case of not voting
* Auditability: It should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records, in terms of physical, permanent audit trail
* Voter Confirmation: The voter shall be able to confirm clearly how his vote is being cast, and shall be given a chance to modify his vote before he commits it.
* Documentation and Assurance: The design, implementation, and testing procedures must be well documented so that the voter-confidence in the election process is ensured.

**Security Requirements**

* Voter Authenticity: Ensure that the voter must identify himself (with respect to the registration database) to be entitled to vote.
* Registration: The voter registration shall be done before voting.
* Voter Anonymity: Ensure that votes must not be associated with voter identity.
* System and Data Integrity: Ensure that the system cannot be re-configured during operation. Ensure that each vote is recorded as intended and cannot be tampered with in any manner, once recorded (i.e., votes should not be modified, forged or deleted without detection).
* Reliability: system should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of network communication. The system shall be developed in a manner that ensures there is no malicious code or bugs.
* Simplicity: The system shall be designed to be extremely simple, as complexity is the enemy of security.