

Biometric based Electronic Voting Machine using Arduino Microcontroller and Fingerprint sensor

Submitted in partial fulfillment of the requirements for the award of Bachelor of
Engineering Degree in Electronics and Communication Engineering

by
LakkimsettiHemanth(37130216)
MadalaAdithya(37130224)



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS
ENGINEERING**

**SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY (DEEMED TO BE
UNIVERSITY)**

**Accredited with Grade “A” by NAAC
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

MARCH 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

www.sathyabama.ac.in



**DEPARTMENT OF ELECTRONICS AND
COMMUNICATION ENGINEERING
BONAFIDE CERTIFICATE**

This is to certify that this Project Report is the bonafidework of **Lakkimsetti Hemanth (37130216)** and **Madala Adithya (37130224)** who carried out the project entitled “**BIOMETRIC BASED ELECTRONIC VOTING MACHINE USING ARDUINO MICROCONTROLLER AND FINGERPRINT SENSOR**” under our supervision from September 2020 to March 2021.

Internal Guide

Dr. G.D. Anbarasi Jebaselvi, M.E.Ph.D

Associate Professor, Department of ECE

Head of the Department

Dr. T. RAVI, M.E.,

Ph.D.

Submitted for Viva voce examination held on _____

Internal Examiner

External Examiner

DECLARATION

We, **Lakkimsetti Hemanth(37130216)** and **Madala Adithya(37130224)** hereby declare that the Project Report entitled “**BIOMETRIC BASED ELECTRONIC VOTING MACHINE USING ARDUINO MICROCONTROLLER AND FINGERPRINT SENSOR**” done by us under the guidance of **Dr. G.D. Anbarasi Jebaselvi, M.E.Ph.D** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

1)

2)

DATE:

PLACE:

SIGNATURE OF THE CANDIDATES

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr. N. M. NANDHITHA, M.E., Ph.D. Dean, School of Electrical and Electronics Engineering** and **Dr. T. RAVI, M.E., Ph.D. Head of the Department, Department of Electronics and Communication Engineering** for providing us necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Dr. G. D. Anbarasi Jebaselvi, M.E. Ph.D** Associate Professor, Department of ECE for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of the project work.

We wish to express our thanks to all teaching and Non-teaching staff members of the **Department of Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

We express our gratitude to our parents for their constant encouragement and support for the completion of the project.

ABSTRACT

Fundamental right to vote or simply voting in elections forms the basis of democracy. One of the key yardsticks used to measure a state's democratic status is the conduct of frequent, competitive, participatory, credible, and nonviolent elections. Since we began practising democracy, elections have been conducted using the manual method of voting, but these elections have been marred by numerous electoral malpractices and glitches. Aggressive attacks on voters, outcome manipulations, vote buying, and the remoteness of polling centres are only a few examples. There are sufficient reasons to justify the creation and implementation of an electronic voting system that addresses the majority of these issues. The e-voting system aims to eliminate the bottlenecks evident in the manual voting system such as the lengthy registration process, unnecessary transportation, election violence and ultimately the incredibility of the votes.

This was accomplished by creating a time-saving registration platform that instantly registers a voter and makes them vote. The voter can also vote at their nearest, secure, and convenient polling station, and their votes will be counted correctly.

In comparison to the manual method, the results of subsequent tests were very impressive in terms of time, security, and accuracy.

Such a system, with all of these capabilities, will go a long way toward alleviating the aforementioned issues with the electoral process' current manual voting system.

Table of Contents

CHAPTER No.	TITLE	PG.NO
	Bonafide	
	Declaration	
	Acknowledgement	
	Abstract	
	List of Tables	1
	List of Figures	2
1	INTRODUCTION	4
1.1	Background of Study	4
1.2	Electronic-voting System Overview	4
1.3	Problem Statement	5
1.4	Aim and Objectives	5
1.5	Significance of the Project	6
1.6	Scope/Limitations of the Work	7
1.7	Project Outline	7
2	LITERATURE REVIEW	9
2.1	Theories of the Technologies Involved	9
2.1.1	Overview of Two-factor Authentication	9
2.1.2	Smart Card Technologies	12
2.1.3	Fingerprint Scanner	15
2.1.4	Database Technologies	20
2.2	Summary of the Reviewed Literature	26
3	METHODOLOGY AND SYSTEM DESIGN	27
3.1	Methodology	27
3.2	Research Purpose	27
3.3	Research Approach	27
3.4	Research Conclusion	27
3.5	Result Interface	29
3.6	Specifications	30

CHAPTER No.	TITLE	PG.NO
3.6.1	16* 2 width LCD Screen	30
3.6.2	Finger print Scanner	30
3.6.3	Arduino UNO	32
4	SYSTEM IMPLEMENTATION AND ANALYSIS	33
4.1	Voting Interface	34
4.2	System Integration and Testing	36
5	CONCLUSION AND RECOMMENDATION	38
5.1	Conclusion	38
5.2	Recomondation	38
5.3	Contribution to knowledge	38
6	REFERENCES	39

LIST OF TABLES

Table 3.1: Recommended LCD Screen 16 * 2 width Specification	31
Table 3.2: Recommended Fingerprint Scanner Specification	31
Table 4.1: Unit test for the LCD screen	34
Table 4.2: Unit test for the Fingerprint Scanner	35
Table 4.3: Overall System Testing	36

LIST OF FIGURES

Figure 2.1: RSA SecurID token, an example of a disconnected token generator	11
Figure 2.2: A Pictorial representation of a Smart Card System ¹⁹	12
Figure 2.3: ISO-7816 standard pin-out of a basic Smart card chip	13
Figure 2.8: A Fingerprint Scanner	15
Figure 2.9: Block Diagram of a Fingerprint System	16
Figure 2.10: Components of the Database Environment	21
Figure 3.1: System Functional Flowchart	29
Figure 3.2: The Result Interface Flowchart	30
Figure 3.3: LCD Display	31
Figure 3.4: Finger Print Display	32
Figure 3.5: The arduino microcontroller	32
Figure 4.1: The Voting Interface Implementation	33
Figure 4.2: Results Displayed on the lcd screen	37

LIST OF ABBREVIATIONS

EVS	-	Electronic VotingSystem
INEC-		Independent National ElectoralCommission
ICT	-	Information CommunicationTechnology
BEME-		Bill of Engineering Measurement andEvaluation
2FA	-	Two-FactorAuthentication
ATM	-	Automated TellerMachine
PIN	-	Personal IdentificationNumber
OTP	-	One TimePassword
GPS	-	Global PositioningSystem
USB	-	Universal SerialBus
PDA	-	Personal DigitalAssistant
ISO	-	International StandardOrganization
IEC	-	International Electrical Community
RFID	-	Radio Frequency Identification
EMV	-	Europay, MasterCard, Visa
APDU-		Application Protocol DataUnit
IAFIS	-	Integrated Automated Fingerprint IdentificationSystem
CASE	-	Computer-Aided SoftwareEngineering
DBMS-		Database ManagementSystem
SQL	-	Structured Query Language
PVC	-	Permanent VotersCard
ATM	-	Automated TellerMachine

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Decisions must be taken between multiple choices in every democratic setting with people with varying and inconsistent opinions. This occurs in the corporate world, the educational world, social organisations, and, most notably, in government. Voting is one of the methods for making such a decision. Voting is a formal mechanism for individuals to show their support or opposition to a motion. This method is often used in the governance field of many organisations to appoint or nominate a chief. Elections are one of the most important fields where voting is used. The formal process of nominating a candidate for public office or endorsing or refusing a political proposal is known as an election.

1.2 Electronic-voting System Overview

E-voting (Electronic Voting) as a term encompasses a broad range of voting systems that apply electronic elements in one or more steps of the electoral cycle. In a broad sense, e-voting can take many forms, including e-collection, e-verification, internet voting, remote online voting, and so on. An e-voting system is any system that can provide both electronic and online voting, according to the concept of a system as something that takes an input and produces an output. E-registration, e-verification, e-collation, remote online voting, and real-time result display may all be included. For an E-voting system (EVS) to work properly, it must have the following components.:

- ❑ An interactive voting user interface on an electronic device which provides a friendly environment for voters to authenticate and cast their votes, it also serves as a means of collection the individual votes and storing them in the local and central database.
- ❑ An administrative dashboard for voters registration, details update and elections coordination and monitoring.
- ❑ A database management system for the storage of election, voting and voters data.
- ❑ A result display interface.

E-voting systems reduce overall election costs and increase voter participation by providing voters with a simple and convenient way to vote. Most importantly, they address the issue of voters travelling long distances to a specific location for their votes to be counted, as well as ballot box snatching, which is common in the United States.

The election process has seen significant technological advancements, especially in the areas of result collation and transmission. Owing to a lack of legislative basis, the Independent National Electoral Commission INEC has not completely incorporated the use of technology for collation. However, ICT is used in most elections around the world to some extent, at least to summarise and aggregate votes. This electronic adaptation is the culmination of a long period of evolution during which not only the processes for casting votes, but also the technical means for doing so, have evolved significantly.

1.3 ProblemStatement

The present voting system applicable in the electoral system has proved inefficient as the voters' registration process is slow, the manual collation of results takes time and gives room for result manipulation, also the inaccessible nature of election venues which includes the long distances to be covered by voters' to their registered location increases. The issues of ballot box snatching and destruction, as well as other election violence and issues associated with conventional ballot paper voting, all taint the intent of voting in an election process as a structured process of expressing individual opinions for or against a motion.

1.4 Aim andObjectives

In the quest to design a successful system to tackle the issues stated in the problem statementThe project's goal and goals are outlined below.

Aim

The aim of this project is to develop and implement a low-cost, real-time automated electronic voting system.

Objectives

Project Objectives includes

1. A detailed study of the election processes as it pertains to voting.
2. Design and develop election voting system that verifies the identity of the voters by their biometric data.
3. Design and develop an electronic device that incorporates fingerprints technology for voters accreditation, authentication and verification.
4. Design and develop an administration dashboard for the election administrators.
5. Run simulations and compare the results of the designed e-voting system

1.5 Significance of the Project

The project's benefits are itemised as follows, in light of the rapid growth of computer technology in practically all fields of activity and its application in relation to knowledge management:

To the University

An e-voting system is beneficial to the university as:

1. It will provide a means to conduct a more less stressful and fair elections at different levels (faculty, departments, school wide e.t.c) in the university.
2. It will offer an in-depth knowledge of the practical approach to ICT education.
3. It will serve as a hands-on application of theories taught in class as it relates to database, software and hardware development.
4. Student and staff information can be conveniently obtained for quick access and tracking since the database is built on a versatile database management framework.
5. Its' smart card system can also be applied to other fields (e.g. networking) for easy access of each individuals' data.
6. It will serve as a base for other works in the field of ICT in governance.

To the Society

The significance of an e-voting system to the society are itemized as follows:

1. It will provide INEC (Independent National Electoral Commission) with a means to conduct less costly and fair elections.
2. The secure and flexible system safeguards data and information to account for credible elections.
3. It will serve to reduce the workload in the process of conducting election.
4. As it incorporates remote voting individuals can vote from their convenience.
5. It will enable INEC reduce the time wasted in collating and announcing election result.
6. It will greatly reduce and eliminate disenfranchising electorates.
7. It will serve to eliminate invalid votes, curb election violence as votes are counted immediately as they are cast.

1.6 Scope/Limitations of the Work

This project's main goal is to encourage the Independent National Electoral Commission to use electronic devices to collect voter information and allow voters to cast votes more easily and comfortably, resulting in a more reliable, successful, and cost-effective election.. The dynamic nature of the elections application interface and database structure allows for different organizations set up and conduct basic elections too. It's online interface enables real-time election monitoring and result collation. Some of its major limitations are:

1. It requires network access: Since the collection and sending of votes to the database requires an internet access which may not be readily available in some urban area would seem a limiting factor, though the local database and the printed vote can be used for counting until network is restored.
2. Setting up an e-voting system is expensive: Due to the fragile nature of such a system and the fact that its major components are currently not available locally, it will be very costly to set up, but its usage and maintenance costs are much lower than the current ballot paper system.
3. It depends on electricity to a point: In as much as it has an in built battery that can last for the required election duration on daily basis, a case of low battery would require it to recharge, which may not be possible if there is no electric power at the moment.

1.7 Project Outline

This project work on e-voting system is made up of five chapters: introduction, literature review, methodology and system design, systems implementation and result analysis, conclusion and recommendation.

In the chapter one of this project, the introduction which briefly explains voting and elections in general, is seen. It goes on to clarify the context of an e-voting system, as well as the system's goal and goals, as well as its meaning, scope, and constraints.

The second chapter dealt with a study of previous literature and the technologies used in e-voting systems. We also looked at the various approaches to e-voting systems, their application, critique, and literature reviews, as well as the various gaps in the current literature.

The block diagram of the project work, the various methodologies used in development stages, and the different phases of the project work, which include analysis, design, microcomputer programming, display programming, testing, and fabrication, are all shown in chapter three. We extensively cover the

requirements of the project, the mathematical models used designs and software incorporated in the work.

In chapter four, we talk about the measures taken and methods used in the project's actual implementation We can see checks being run to ensure that the project is running smoothly, as well as the results and their importance. We can also see the challenges that have been faced, as well as the methods and solutions that have been used to solve them or not.

And finally, in chapter five, we conclude the work and give notable recommendations for optimal operation of the product. Also we provide suggestions for improvement, enhancement and optimization of our existing work. We also outline the major contribution to the body of knowledge in which our work has achieved.

CHAPTER 2

LITERATURE REVIEW

2.1 Theories of the TechnologiesInvolved

2.1.1Overview of Two-factorAuthentication

Two-factor authentication (also known as 2FA) is a form of multi-factor authentication, or a subset of it. Multi-factor authentication is a type of machine authentication in which a user is granted access after successfully presenting two or more pieces of evidence (or factors) to an authentication device, such as knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user has) (something the user and only the user has) (something the user and only the user is).

As a result, 2FA is a method of verifying users' asserted identities by combining two factors: 1) what they know, 2) something they have, or 3) what they are. Withdrawing money from an ATM is a clear example of two-factor authentication; the transaction can only be completed with the right combination of a bank smart card (something the user has) and a PIN (something the user knows). Another example is to use a one-time password (OTP) or a code created and obtained by the user (e.g. a security token) on a smartphone that only the user has access to.

Two-step verification, also known as two-step authentication, is a method of verifying a user's assumed identity by using something they know (password) and a second factor other than something they have or are. A user repeating back something that was sent to them via an out-of-band process is an example of a second phase. A six-digit number provided by another system that is shared by the user and the authentication system may also be used as the second stage.

AuthenticationFactors

Since an unauthorised actor is unlikely to be able to supply the factors required for entry, multiple authentication factors are used to prove one's identity. (e.g a building, or data,)

The user is then blocked despite being secured by multi-factor authentication. A multi-factor authentication scheme's authentication factors may include:

- ② some physical object in the possession of the user, such as a USB stick with a secret token, a bank smart card, a key, etc.
- ② some secret known to the user, such as a password, PIN, TAN etc.
- ② some physical characteristic of the user (biometric), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.
- ② somewhere you are, such as connection to a specific computing network or utilizing a GPS signal to identify the location.

The above authentication factors are further discussed under the following sub headings:

1. Knowledge Factors
2. Possession Factors
3. Inherent Factors
4. Location Based Factors

Knowledge Factors: are the most widely used authentication method. In order to authenticate, the user must prove knowledge of a secret in this form. A password is a hidden word or string of characters used to verify the identity of a user. This is the most widely used authentication method. Passwords are used as one aspect of authentication in many multi-factor authentication techniques. [nine] Longer personal identification numbers (passwords) and shorter, strictly numeric personal identification numbers (PINs) are widely used for ATM entry. Passwords are traditionally meant to be memorised. Many hidden questions, such as "Where were you born?" are poor examples of intelligence factors since they could be identified by a large number of people or could be studied.

Possession Factors: (defined as "something the user and only the user has") have been used for authentication in the form of a key to a lock for centuries. The basic principle is that the key encapsulates a secret that is exchanged between the lock and the key, and possession factor authentication is based on the same principle.

in terms of operating systems. A security token is an example of a possession factor. Possession factors

could be grouped as follows:

- i. Disconnectedtokens.
- ii. Connectedtokens.
- iii. Software tokens.

Disconnected tokens have no connections to the client computer. They typically use a built-in screen to display the generated authentication data, which is manually typed in by the user.[12]



Figure 2.1: RSA SecurID token, an example of a disconnected token generator

Tokens that are physically attached to the machine to be used are known as connected tokens. These devices automatically transmit data. (#13) Card readers, wireless tags, and USB tokens are all examples of various styles.[13]

A software token (also known as a soft token) is a two-factor authentication protection device that can be used to authorise access to computer services. Software tokens can be duplicated and placed on a general-purpose electronic device like a desktop computer, laptop, PDA, or cell phone. (This is in contrast to hardware tokens, which store credentials on a dedicated hardware device and therefore cannot be duplicated unless the device is physically invaded.) A soft token may or may not be a system with which the user communicates. To serve this function, an X.509v3 certificate is usually loaded onto the computer and securely stored..

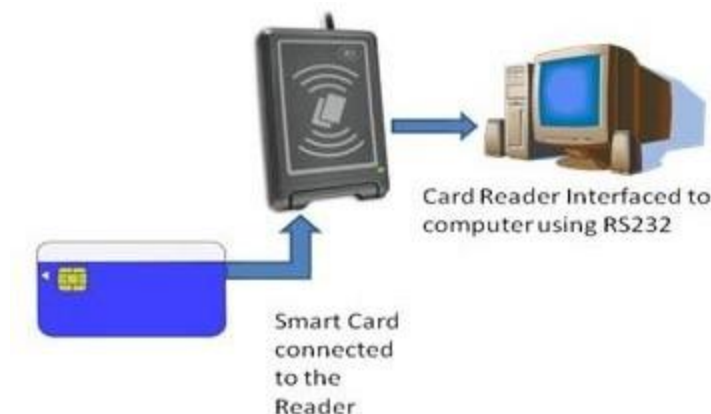
Inherent Factors: are factors associated with the user, and are usually biometric methods, including fingerprints, face, voice, or iris recognition. Behavioral biometric such as keystroke dynamics can also be used.

Location Based Factors: A fourth element, the user's physical position, is increasingly coming into play. A user could be able to authenticate using only a pin code when hardwired to the corporate network, but while off the network, a code from a soft token could be needed as well. When access to the office is regulated, this may be considered an appropriate norm. Network admission control systems operate in a similar manner, with the level of network access being determined by the network to which your computer is linked, such as WIFI vs wired connectivity. This also enables a user to switch between offices while maintaining the same degree of network access.

Authentication is a critical security feature in applications, and it can be improved with two-layer authentication to increase confidence in the system's overall integrity.

2.1.2 Smart Card Technologies

A smart card, also known as a chip card, is a plastic card with an embedded computer chip—either a memory or a microprocessor—that stores and transmits data. This information is normally associated with either a monetary value, information, or both, and is stored and processed inside the card's chip.



The information on the card is transferred using a reader that is part of a computer system.

Figure 2.2: A Pictorial representation of a Smart Card System

Smart card-enabled systems are currently in use in a variety of industries, including healthcare, banking, governance, entertainment, and transportation. Smart cards can support both of these applications by providing additional features and protection. Smart cards are a type of machine-readable card that is used for authentication. Markets that have previously been served by other machine-readable card technologies, such as bar-code and magnetic stripe, as well as traditional authentication methods, such as passwords and forms, are converting to smart cards as the measured

return on investment is revisited year after year by each card issuer. ISO/IEC is a global standard-setting organisation for technology, which includes plastic chip cards. ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693, and ISO/IEC 7501 are the most common smart card standards. The physical dimensions, electrical interface, communication protocols, and database structure approach are all described by these principles. A smart card system is made up of two parts: the smart card and the card reader.



Figure 2.3: Standard pin-out of a simple Smart card chip according to ISO-7816.

The Smart CardChip

To bear the electronic chip, the smart card uses the same basic plastic media as magnetic stripe-based cards: To bind the silicon to the outside world, eight gold-plated contacts are used..As shown in figure 2.3, these contacts are arranged according to the ISO7816-1 specification.

Description of Smart CardPin-out

1. C1 (VCC +5V DC): Input power supply (optional use by the card)
2. C2 (RESET): Reset signal, which is used to clear the card's communications.
3. C3 CLOCK : Provides the card with a clock signal, from which data communications timing is derived
4. C4 (RESERVED AUX1): Optionally used for USB interfaces and other uses.

5. C5 (GND): Ground (reference voltage)
6. C6 (Vpp): Voltage input programming (optional). This touch can be used to provide the voltage needed to programme or delete the non-volatile memory within the device. This was designated as a programming voltage in ISO/IEC 7816-3:1997: an input for a higher voltage to programme permanent memory (e.g., EEPROM). It is designated as SPU in ISO/IEC 7816-3:2006 for regular or proprietary use as input and/or output..
7. C7 (I/O) : Input or Output for serial data (half-duplex) to the integrated circuit inside the card.
8. C8 (RESERVED AUX2): Optionally used for USB interfaces and other uses.

Advantages of SmartCards

1. Smart cards can have a higher degree of protection than magnetic stripe cards since they contain microprocessors that can process data without the need for external connections.
2. Smart cards are typically made of plastic, generally polyvinyl chloride and are of dimension 85.60 by 53.98 millimeters, which makes them portable and very easy to carry about.
3. Another advantage of smart cards is that once information is stored on a smart card, it can't easily be deleted, erased or altered. As such, smart cards are good for storing valuable data that can't be -- or shouldn't be -- easily reproduced.
4. Smart card technology is generally safe against electronic interference and magnetic fields, unlike magnetic stripe cards. In addition, applications and data on a card can be updated through secure channels so issuers do not necessarily have to issue new cards when an update is necessary.
5. Multi-service smart card systems can enable users to access more than one different service with just one smartcard.
6. The cost a smart card is very affordable and it is not costly to implement and manage.

Disadvantages of SmartCards

1. While smart cards have many advantages, the cards themselves -- as well as the smart card readers -- can be expensive as it is not locally sourced in at the moment.
2. Another drawback to smart cards is that not all smart card readers work for all smart card forms. Some smart cards and readers use proprietary software that is incompatible with other

readers, and some smart cards and readers use nonstandard protocols for data storage and card interface.

3. Although smart cards are more secure in many applications, they are still susceptible to certain attacks. Smart card technology is vulnerable to attacks that can retrieve information from the chip. The on-chip private key used by public key algorithms can be deduced using differential power analysis. Some symmetric cypher implementations are also vulnerable to timing attacks and differential power analysis.
4. Smart cards may also be physically disassembled in order to gain access to the on-board microchip.

The automatic method of verifying a match between two human fingerprints is known as fingerprint recognition or fingerprint authentication. An ink-less scanner is usually used to obtain a better print impression. In terms of ridge bifurcations and ridge endings, the digital image of the fingerprint contains many special features known as minutia [19].

2.1.3 FingerprintScanner

A fingerprint scanner is a computer that captures a digital image of a person's fingerprint pattern. The comparison of several features of the print pattern is usually needed when analysing fingerprints for matching purposes. Patterns, which are ridge aggregate characteristics, and minutia points, which are unique features found within patterns, are examples.



Figure 2.8: A Fingerprint Scanner

Parts of a FingerprintScanner

The fingerprint scanner consists of fingerprint sensor, ADC (Analog to Digital Converter), flash ROM and DSP (Digital Signal Processing) chip.

1. **Fingerprint Sensor:** The fingerprint sensor is used for scanning the finger impression. The scanning data is in the form of analog. Further, this process is converted by the A/D converter.
2. **A/D Converter:** Here the analogue data from the sensor is converted to the digital data and it is transferred to the processor.
3. **Flash ROM:** The flash ROM is used to store the data temporarily in the DSP processor and this will work until the data is transferred to the main memory of the host.
4. **DSP Chip:** The DSP chip is used for processing and receiving the data. For further transfer of data the DSP port is used.
5. **DSP Port:** It is used for the communication between DSP processor and memory (database).

Components of a Fingerprint System

A typical fingerprint system consists of four major components, which consist of:

1. Image capture
2. Feature extraction
3. Pattern matching
4. Database

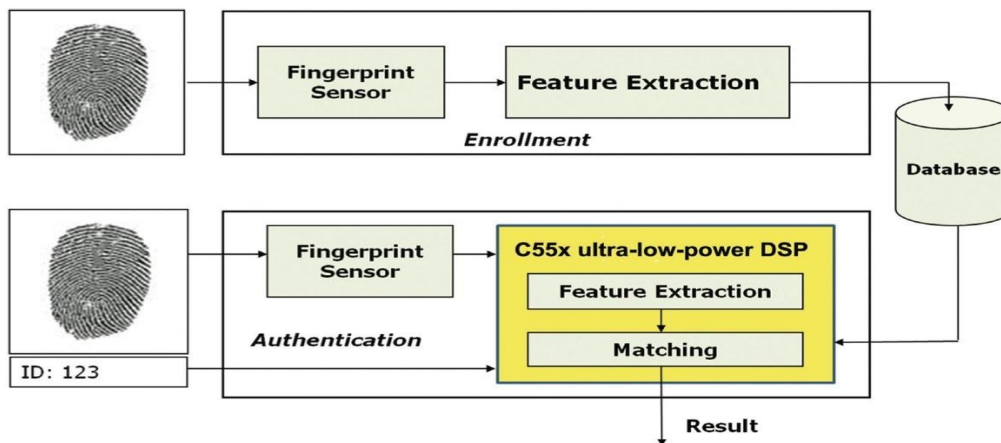


Figure 2.9: Block Diagram of a Fingerprint System [20].

Fingerprint systems convert illuminated fingerprint images into digital code, which is then used by other software for enrollment (fingerprint registration) and verification (authentication or verification of registered users). The scanner captures high contrast, high resolution fingerprint images that are practically distortion-free using an advanced CMOS image sensor. A series of sophisticated algorithms extract data from the image, mapping the fingerprint's distinguishing characteristics.

This information is then translated into a digital template, which is an encoded binary string that is saved in a database. The fingerprint picture itself is never saved. A patented matching algorithm compares the new prototype made from the extracted characteristics from the input fingerprint on the optical module to a previously stored sample to recognise or validate a fingerprint. It takes about a second for the entire matching process to complete. Depending on the system setup, authentication takes place locally on the client or remotely on a server. [20].

Mode of Operation of a FingerprintSystem

A fingerprint biometric system can operate in two modes:

Verification mode: The system performs a one-to-one (1:1) comparison of a captured fingerprint with a specific template stored in the database in order to verify the individual is the person they claim to be.

1. Identification mode: The system performs a one-to-many (1:N) comparison against fingerprints in the database in an attempt to establish the identity of an unknownindividual.

Applications of Fingerprint BiometricTechnologies

There are numerous applications for the use of Biometric Technology, but the most common ones are asfollows:

1. Logical Access Control: This refers to gaining access to a computer network either at the place of the business or corporation or via a secured remote connection from a distant location. Fingerprint systems are deployed to allow for easy access for authenticatedusers.
2. Physical Access Control: refers to giving a person or an employee of a business or a corporation access to a secure building, or even a secure office from within it. Fingerprint systems are installed at entrance points to grant entrance access to only authentic employers or person with such access orclearance.
3. Time and Attendance: Here, fingerprint biometric is used to take records of attendance of the

members of an organisation. The time of arrival and departure can also be recorded and stored in a database for reference purposes.

4. Law Enforcement: This is the most widely known application of fingerprint biometric technologies. Here law enforcement agencies implement fingerprint biometric system as a means of collecting identities of criminals. IAFIS (Integrated Automated Fingerprint Identification System), a worldwide database of fingerprints of criminals is an example of such. IAFIS administrated and maintained by the FBI (Federal Bureau of Investigation) in the United States[21].
5. Surveillance: This is simply keeping tabs of a large group of people, and from there, determining any abnormal behavior from an established baseline. Fingerprint systems are deployed also with face recognition to track for example people with criminal records any erratic behavior.

Advantages of Fingerprints Technologies

1. Fairly small storage space is required for the biometric template, reducing the size of the database required.
2. It is one of the most developed biometrics.
3. Each and every fingerprint including all fingers are unique, even identical twins have different fingerprints and as such it is a safe way of identifying individuals.
4. Sound potential for forensic use as most of the countries have existing fingerprint databases.
5. Relatively inexpensive and offers high levels of accuracy.

Disadvantages of Fingerprints Technologies

1. Even with its many benefits, fingerprint systems are also associated with some disadvantages that makes their implementation controversial, and they include:
 1. The fingerprint scanner does not take into consideration when a person physically changes. Changes such as growth tends to change fingerprints and accidents such as bruises or cuts or even dirt on the finger can make an already existing user's verification invalid as the fingerprint is now altered.
 2. For some people it is very intrusive, because is still related to criminal identification.
 3. If anyone can access to an authorized user's prints, he can trick the scanner. The criminal can cut off somebody's finger to get a scanner security system but some scanners have additional pulse and heat sensors to verify that the finger is alive, but these systems can still be fooled by a gelatin print mold over a real finger[22].
 4. Having a high security system may require expensive computer hardware and software, certain fingerprint scanners can be quite expensive.

Fingerprint authentication is the cheapest, fastest, most convenient and most reliable way to identify a particular person. It has many functional advantages over traditional systems such as passwords. The greatest strength of the fingerprint authentication technology, is the fact that the fingerprint does not change over time.

Today, fingerprint recognition technology is used for mostly security and identification purpose. As

fingerprint recognition technology advances, more affordable and compact fingerprint recognition devices are expected to become available, and fingerprint recognition will be regarded as a safe and convenient authentication method.

2.1.4 Database Technologies

At the heart of every fully designed system are the collection, storage, aggregation, manipulation, dissemination, and management of data [23]. **Data** are raw facts. The word raw indicates that the facts have not yet been processed to reveal their meaning. **Information** are data that have been processed in such a way that the knowledge of the person who uses the data is increased. These facts are made available for processing because they are stored at a place for future reference. The two main techniques for data storage in computers are: file system and database.

A file system is a method of storing and organising computer files and the data they contain in such a way that they are easy to locate and access. File systems use a storage unit such as a hard disc or CD-ROM to keep track of where the files are physically located. A file system can be used to store less complex data, but storing an organization's data, such as employee information, financial records, and so on, requires a well-structured system, which is referred to as a database.

Database is as an organized collection of logically related data. It is a collection of data, typically describing the activities of one or more related organizations. A database can also be seen as a shared, integrated computer structure that stores a collection of:

- ❑ End-user data, that is, raw facts of interest to the enduser.
- ❑ Metadata, or data about data [23], through which the end-user data are integrated and managed.

The file systems became obsolete as their integration and use becomes difficult when the volume of data stored increases. Its numerous disadvantages led to the development of database as an easier means for data storage, but as the need for a good data manipulation system increased, there was need to develop a management system for databases for quick access and control and that gave rise to the Database Management System(DBMS).

Components of the Database Environment

The database operational environment shown in Figure 2.10 is an integrated system of hardware, software, and people, designed to facilitate the storage, retrieval, and control of the information resource and to improve the productivity of the organization. They are includes:

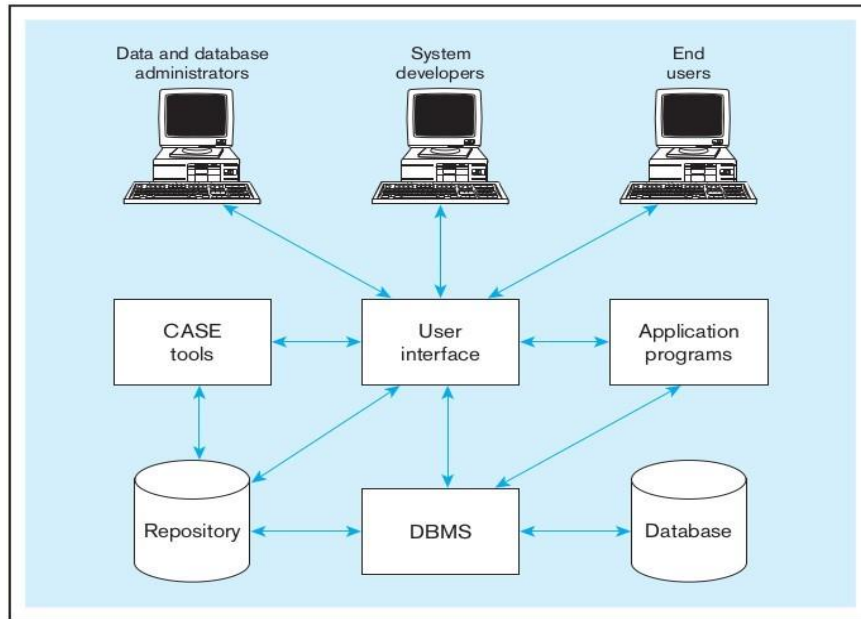


Figure 2.10: Components of the Database Environment [24].

Computer-aided software engineering (CASE) tools: CASE tools are automated tools used to design databases and application programs.

Repository: A repository is a set of metadata that is useful for maintaining databases and other information system components.

DBMS: It's a software framework for creating, maintaining, and controlling access to user databases.

Database: It is a logically linked set of data that is structured to satisfy the information needs of different users in an organisation. It's important to understand the difference between a database and a repository. Data descriptions are stored in the archive, while data events are stored in the database.

Application programs: The database is created, maintained, and information is provided to users using computer-based application programmes.

User interface: This includes languages, menus, and other facilities by which users interact with various system components, such as CASE tools, application programs, the THINGSSPEAK DATABASE, and the repository.

Data and database administrators: Data administrators are tasked with overseeing the management of an organization's data resources. Database managers are in charge of the physical design of databases as well as the management of technical problems in the database system.

System developers: They are people who develop new application programmes, such as systems analysts and programmers. CASE techniques are often used by system developers for system requirements analysis and software design.

End users: These are the people who add, remove, and change data in the database, as well as those who request or obtain information from it. The THINGSSPEAK DATABASE must handle all user interactions with the database..

Database ManagementSystem

A database management system (DBMS) is a piece of software that allows you to use a database. The primary goal of a THINGSSPEAK DATABASE is to provide a standardised method for generating, modifying, storing, and extracting data from a database. It allows end users and application programmers to exchange data and to share data across different applications rather than propagating and storing data in new files for each new application [24]. Controlling data access, enforcing data integrity, managing concurrency control, and restoring a database are all possible with a THINGSSPEAK DATABASE.

There are many terms associated with the THINGSSPEAK DATABASE used to explain the different operations in a database environment, they includes terms like query -- a specific request issued to the THINGSSPEAK DATABASE for data manipulation — for example, to read or update the data. Simply put, a query is a question.

The terms database and THINGSSPEAK DATABASE are most times used interchangeably to refer to the database technology and as such we adopt such use here to us focus on the technological aspects of the database approach.

Advantages ofDatabase

As a database is only as useful as its THINGSSPEAK DATABASE , the advantages of a THINGSSPEAK DATABASE are as follows:

1. Improved data sharing: The THINGSSPEAK DATABASE helps create an environment in which end users have better access to more and better-managed data. Such access makes it possible for end users to respond quickly to changes in their environment.
2. Improved data security: The more users access the data, the greater the risks of data security breaches. Corporations invest considerable amounts of time, effort, and money to ensure that corporate data are used properly. A THINGSSPEAK DATABASE provides a framework for

better enforcement of data privacy and security policies.

3. Better data integration: Wider access to well-managed data promotes an integrated view of the organization's operations and a clearer view of the big picture. It becomes much easier to see how actions in one segment of the organisation affect other segments.
4. Minimized data inconsistency: Data inconsistency exists when different versions of the same data appear in different places. For example, data inconsistency exists when a company's sales department stores a sales representative's name as "MaryBlessing" and the company's personnel department stores that same person's name as "Mary-Blessing C.," or when the company's regional sales office shows the price of a product as #4,500 and its national sales office shows the same product's price as #4,490. The probability of data inconsistency is greatly reduced in a properly designed database.
5. Improved data access: The THINGSSPEAK DATABASE makes it possible to produce quick answers to ad hoc queries
 - a spur-of-the-moment question [23]. The THINGSSPEAK DATABASE sends back an answer (called the query result set) to the application. For example, end users, when dealing with elections data, might want quick answers to questions (ad hoc queries) such as:
 - ☐ What was the total number of registered voters during the past six months?
 - ☐ What is the total number of students who can vote?
 - ☐ How many candidates are contesting for a particular election?
6. Improved decision making. Better-managed data and improved data access make it possible to generate better-quality information, on which better decisions are based. The quality of the underlying data determines the quality of the information produced. Data quality refers to a holistic approach to ensuring data accuracy, validity, and timeliness. While the THINGSSPEAK DATABASE does not guarantee data consistency, it does provide a forum for data quality measures to be implemented.
7. 7. A boost in end-user efficiency. End users can make fast, informed decisions based on the availability of data and the tools that turn data into usable knowledge, which can mean the difference between success and failure in the global economy.
8. Greater data independence: Application systems should be as unaffected by data representation and storage information as possible. To protect application code from such information, the THINGSSPEAK DATABASE may provide an abstract view of the data.

Disadvantages of Database

The database approach entails some additional costs and risks that must be recognized and managed when it is implemented.

1. 1. Need for new, specialised personnel: Companies that follow the database approach often need to recruit or train people to develop and implement databases, provide database management services, and manage a team of new people.
2. Installation and management cost and complexity: Installing such a system may also require upgrades to the hardware and data communications systems in the organization. Substantial training is normally required on an ongoing basis to keep up with new releases and upgrades. Additional or more sophisticated and costly database software may be needed to provide security and to ensure proper concurrent updating of shared data.
3. Costs of conversion: The cost of converting these older systems to modern database technology, measured in terms of resources, time, and organisational effort, can be prohibitive for a company.
4. 4. The need for explicit backup and recovery: This necessitates the creation and implementation of robust protocols for providing data backup copies and restoring databases when damage occurs.
5. Organizational conflict: Disputes over data definitions, data formats and coding, rights to update shared data, and related issues are common and difficult to address, according to experience.

Types of Database

Depending upon the usage requirements, there are following types of databases available:

1. Centralized database: Information (data) is stored in a centralised location and can be accessed by users from various locations. This database form includes application procedures that enable users to access data from a remote location. End users are verified and validated using a variety of authentication procedures, and application procedures include a registration number that is used to keep track of and monitor data use.
2. Distributed database: The data is spread through many locations within an entity. These sites are linked together by communication connections, allowing them to easily access the distributed data. Homogeneous and heterogeneous distributed databases are the two types of distributed databases. Homogeneous DDBs are databases that have the same underlying hardware, run on the same operating systems, and use the same application procedures.

Whereas, at different sites of a DDB, the operating systems, underlying hardware, and application procedures may be different, which is known as heterogeneousDDB.

3. Personal database: Data is collected and stored on portable, easy-to-manage personal computers. The data is usually only viewed by a select number of people and is used by the same department of an organisation.
4. End-user database: The end user is normally unconcerned with the transactions or operations carried out at different levels, and is only concerned with the product, which may be software or an application. As a result, much like various levels'managers, this is a shared database that is explicitly developed for the end user. This database contains a summary of all facts.
5. Commercial database: These are the paid versions of large databases created specifically for people seeking information for assistance. These databases are subject-specific, and no one can afford to have such a large amount of data on hand. Commerciallinks are used to gain access to such databases.
6. 6. NoSQL database: This type of database is used to store vast amounts of distributed data. Some big data performance problems are effectively solved by relational databases; however, NoSQL databases can easily handle such issues. They are very effective at processing vast amounts of unstructured data that could be stored on several cloud virtual servers. MongoDB is an example of a NoSQL database. [25].
7. 7. Operational database: This database stores information about an organization's activities. Such databases are needed by functional lines such as marketing, employee relations, and customer service, among others.
8. 8. Relational database: These databases are divided into categories by a collection of tables in which data is classified. The table is made up of rows and columns, with each column containing data for a specific category and each row containing an instance of that data identified by the category. The Structured Query Language (SQL) is a relational database's standard user and application software interface.

There are a number of basic operations that can be performed on a table, making it simpler to expand these databases, join two databases with a similar reference, and change all existing applications.

9. Cloud database: Data is increasingly being processed in databases, also known as virtual environments, whether in a hybrid cloud, public cloud, or private cloud. A cloud database is

one that has been optimised or developed specifically for use in a virtualized environment. A cloud database has many advantages, including the ability to pay for computing space and bandwidth on a per-user basis, as well as scalability on demand and high availability.

A cloud database also gives enterprises the opportunity to support business applications in a software-as-a-service deployment.

10. 10. Object-oriented database: An object-oriented database is a combination of relational databases and object-oriented programming. While there are some items generated with object-oriented programming languages such as C++ and Java that can be stored in relational databases, object-oriented databases are better suited for those items.

Objects, rather than behaviour, and data, rather than logic, are the building blocks of an object-oriented database. A multimedia record in a relational database, for example, may be a definable data object rather than an alphanumeric attribute.

11. Graph database: The graph is made up of nodes and edges, with each node representing an individual and each edge describing the relationship between them. A graph-oriented database, also known as a graph database, is a type of NoSQL database that stores, maps, and queries relationships using graph theory. The main purpose of graph databases is to analyse interconnections. Companies may, for example, use a graph database to mine data from social media to learn more about their customers.

2.2 Summary of the Reviewed Literature

The e-voting systems we reviewed above were all developed out of a quest to enhance the voting systems to meet the recent technological frame and as well provide a means to uphold a credible election. The different e-voting systems have different levels of adoption of technology in them as seen fit by the authors and the users.

Some e-voting systems use a single device with different authentication technology, while some implement two or more devices for authentication and vote casting purposes. Based on the technology available and the interest of the users, an e-voting device that works well is developed and there is always room for constant upgrade and development as technology advances.

The common criticism about the e-voting system is the issue of software security [32], and this has posed a serious threat to the adoption of an e-voting system. In the quest to add a physical assurance to

the e-voting systems, the VVPAT (Voter Verifiable Paper Audit Trail) was advocated to be adopted to allow for manual counting of votes also at the end of the election.

LiteratureGaps

The concept of e-voting systems has its focus on eliminating the issues of multiple voting and other election malpractice associated with the conventional ballot paper voting. Though many works have been done on the area of e-voting and many countries has adopted it for different levels of election, none of them was designed to completely captured the election process. The solution to the issues of voters traveling from one location to another where their vote would count on the Federal level elections is one missing puzzle to the existing e-votingsystems.

CHAPTER 3

METHODOLOGY AND SYSTEM DESIGN

3.1 Methodology

Methodology is the systematic, theoretical analysis of the methods applied to a field of study. The aim of this chapter is to give an introduction about the general research methodology and waterfall methodology for development used in this project.

3.2 Researchpurpose

In the information age, it seems that the use of information technology is an unavoidable trend for the evolution of organisations in the twenty-first century, whether public or private. Electronic democracy, which is governance-oriented, and e-government, which is service-oriented, are two examples of information technology's application in public affairs. E-voting, as a critical component of e-Government systems, would inevitably contribute to the use of information technology to increase the performance of the public sector and citizen engagement through electronicforums.

The purpose of this research is to identify the factors affecting the election process and ways they can be eliminated.

3.3 Researchapproach

There are two main research approaches used in scientific work, quantitative and qualitative. The main difference between these two is that the aim of quantitative research is to find explanation to a phenomenon or a situation that can be generalized to other people and places while in qualitative research the aim is to gain deeper understanding of a phenomena or a situation.

Quantitative approach will be used to discover the issues that threatens the election as it relates to voters.

We are making use of existing data already collected by previous literature on elections to analyze the election process and derive a conclusion on how to eliminate the issues.

3.4 Research conclusion

Based on the reviewed data collected on previous conducted elections, the main issue with the election was the issue of voters apathy towards the electoral system which is as result of

many factor such as inaccessible registration and voting venue, election violence that could lead to loss of lives, result manipulation and so on.

A system that serves to increase voters participation in the electoral process is the remedy to these issues at hand.

E-voting system serves to provide a remedy for the inaccessible registration and voting venue as eligible citizens can be registered and vote at their place of residence for their votes to count for their particular place of origin. It also provides a means to eliminate ballot box snatching as votes are counted as they are cast. There is also less room for result manipulation because the result get updated and displayed to all as votes are beingcounted.

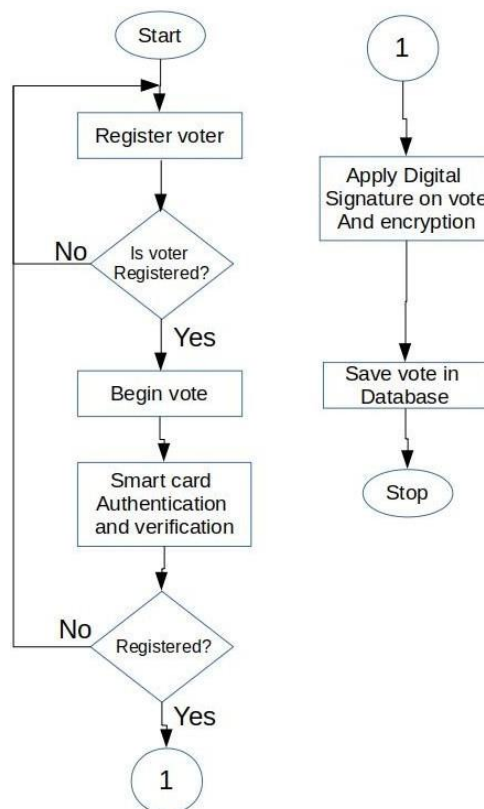


Figure 3.1: System Functional Flowchart

3.5 Result Interface

The result interface design is such that anyone can have access to election results, hence no authentication is required to access this service. Nevertheless, data is transmitted over secure protocols to insure integrity of the results being shown. The interface makes use of bar graphs and chats to show live election results. The result interface program flowchart is shown below.

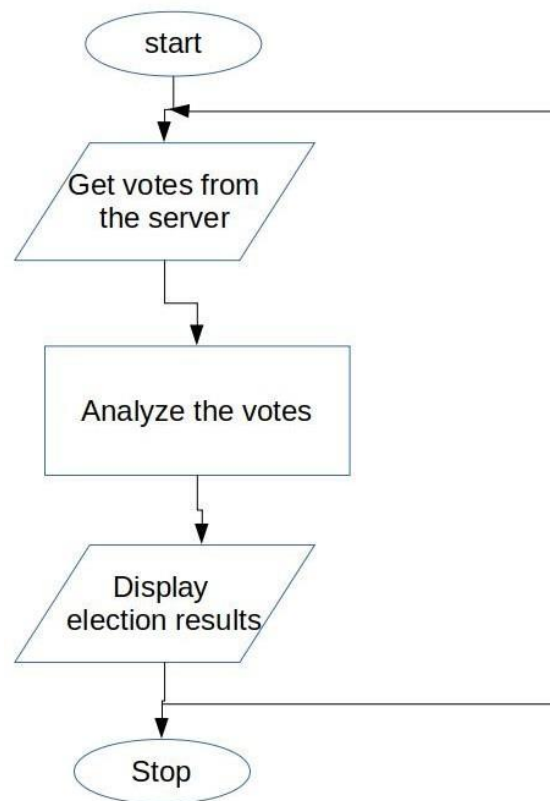


Figure 3.2: The Result Interface Flowchart

3.6 Specifications

3.6.1 16 * 2 width LCD Screen

The screen 16 * 2 width is a resistive LCD screen with a touch controller. The controller renders the graphics output of the arduinouno to the screen 16 * 2 width while sending touch responses from the screen to the arduinouno. The screen 16 * 2 width has an impressive response time and the Table

3.1: Recommended LCD Screen 16 * 2 width Specification

Property	Value
LCD size	16'' inch
Power supply	5V-12V DC
Display size	7~10 inch
Screen type	Resistance screen
LCD resolution	800*480

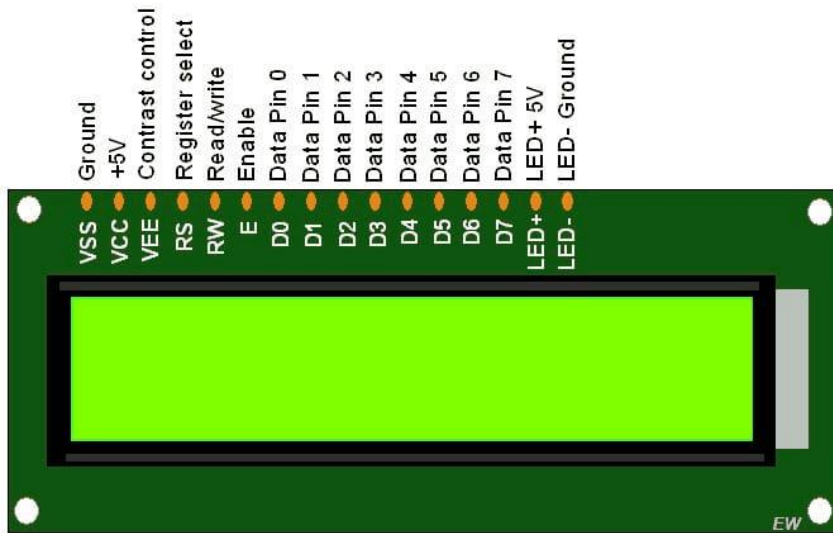


Figure 3.3: LCD Display

3.6.2 FingerprintScanner

This is one out of the two factors of authentication for the voting device, providing strong security and confidence on a voter's vote. The fingerprint scanner enables the fingerprint of the voter to be read for verification or identification of the voter.

Table 3.2: Recommended Fingerprint Scanner Specification

Property	Value
Interface	UART (TTL)

Voltage	4.2-6.0V DC
Resolution	508 DPI
Sensing area	160*160 pixel
Fingerprint capacity	200
Module Size	33.4*20.4 mm

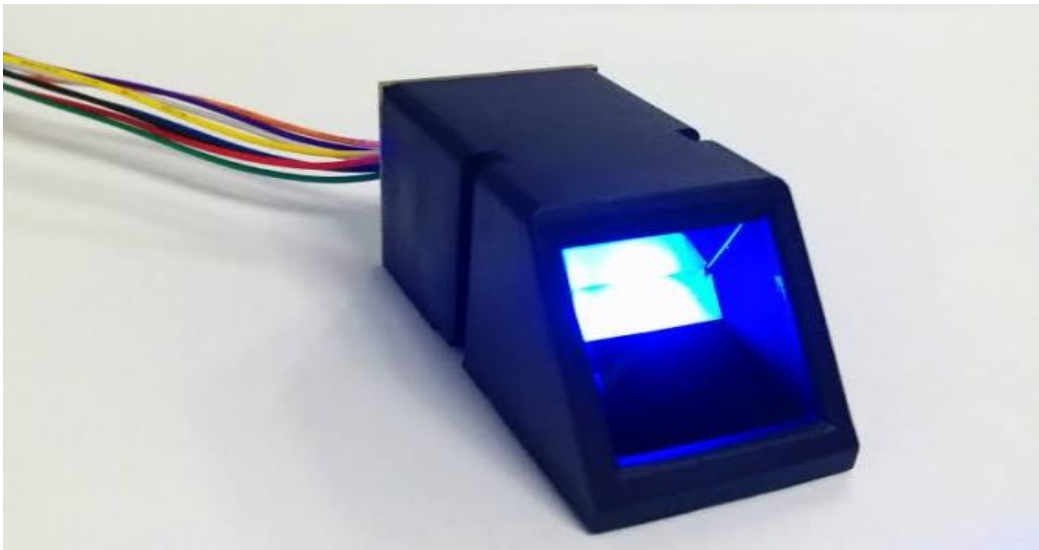


Figure 3.4: Finger print sensor

3.6.3 Arduino UNO:

The **ArduinoUno** is an open-source microcontroller board based on the Microchip ATmega32P microcontroller. The board has a number of digital and analogue input/output (I/O) pins that can be used to connect to different expansion boards (shields) and other circuits. A cpu, another Arduino/Genuino board, or other microcontrollers can all be communicated with using the Arduino/Genuino Uno.

Figure 3.5: The Arduino Microcontroller



CHAPTER 4

SYSTEM IMPLEMENTATION AND RESULT ANALYSIS

4.1 VotingInterface

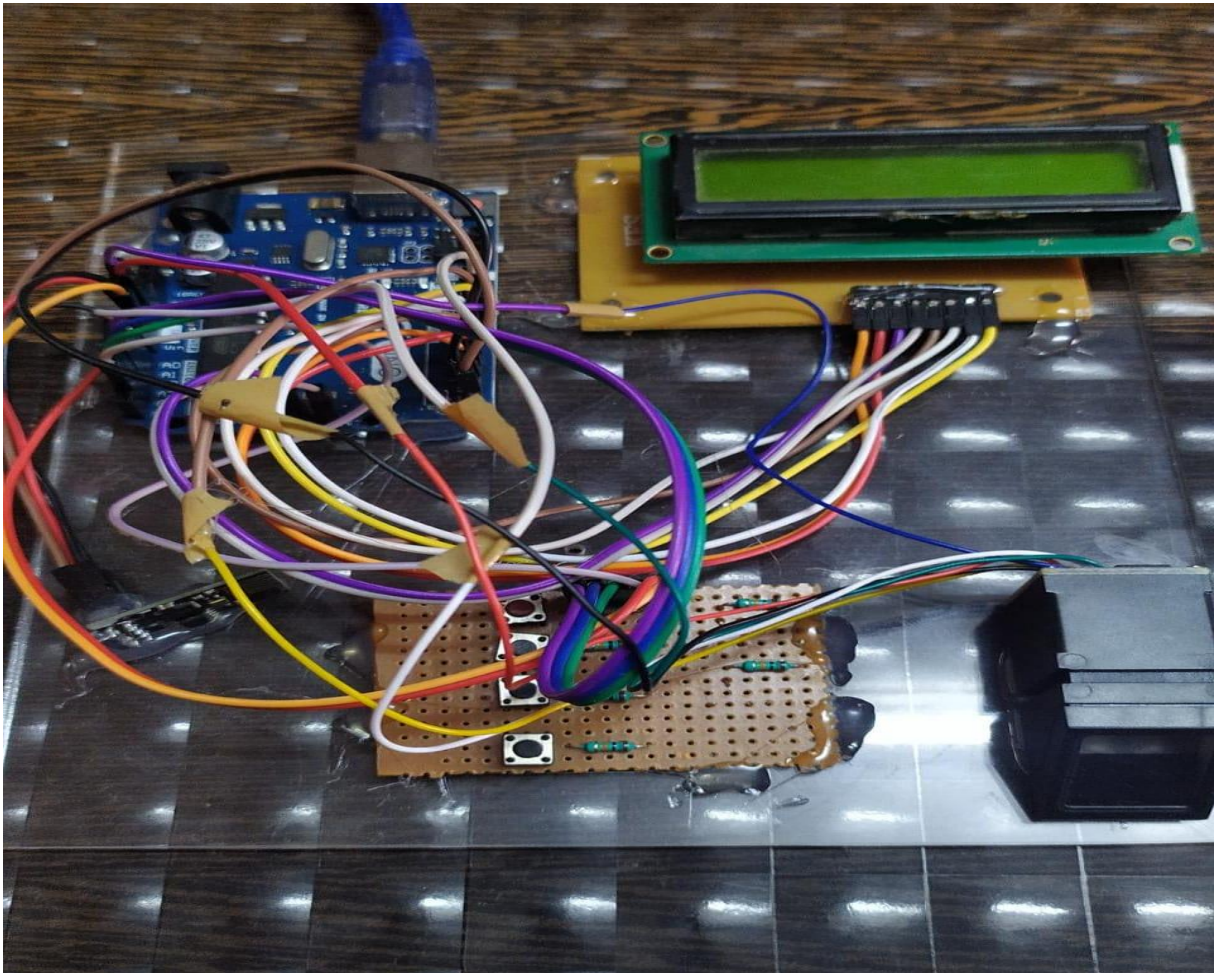


Figure 4.1: The Voting Interface Implementation

PowerUnit

This generates the power required for the devices to operate in a good working condition. It also powers some LEDs for indication purposes. It contains a 12V battery to supply power to the devices in the absence of external power.

The input to the power unit is a 220V AC which is stepped down and converted to DC. This output is used to power the screen 16 * 2 width module and the arduinouno.

LCD Screen

The LCD screen provides a means of interacting with the device. Its powered directly by a 5V power supply from the power unit.

The screen 16 * 2 width is connected to the arduinouno via an HDMI cable for receiving video streams from the arduinouno for display and a USB cable for transmitting input received from user touch to the arduinouno. The controller directly communicates with the arduinooperating system running on the arduinouno enabling input to the screen sensor to be interpreted properly.

Control Unit

The control unit is the heart of the system. It is a arduinouno software. The operating system provides the resources necessary to generate a graphical user interface for the application. It also provides low level libraries to enable easy integration with other peripheral (hardware) devices.

It communicates with the card reader, the fingerprint sensor and the screen 16 * 2 width via its USB ports which serves as a source of power to some of the peripherals like the fingerprint and the card reader.

The voting application or software written in java and python, runs on this operating system and communicates with the peripheral devices by using the low level libraries provided by the operation system.

Table 4.1: Unit test for Control Unit

Test	Steps	Expected Result	Test Result
Arduinouno power	Plug the arduinouno power cord to a power source	The LED on the arduino should come on	The LED came on

Arduinouno OS boot	Put the hdmi cable in the arduinouno and power on the arduinouno	The LED on the arduinouno should come on	TheLEDcame on
Start Application	Attempt to run the vote application	The application should run without errors	The application ran without errors

FingerprintScanner

This is the second means by which the system authenticates a voter. It exposes four pins of which two (the RX and TX) are for serial TTL communication while the other two provides the power supply. The fingerprint sensor is connected to the arduinouno USB port through a TTL-USB converter which also provides enough voltage (5V) to power it. The fingerprint sensor is controlled by a python program which provides a wrapper for the low level libraries that communicates with it. The codes used for this communication is found in the appendixC.

Table 4.2: Unit test for the Fingerprint Scanner

Test	Steps	Expected Result	Test Result
Correct connection	Connect the pins of the finger print scanner to the appropriate pins of the arduinouno	The LED fingerprint scanner should blink .	The LED of the fingerprint blinked .

4.2 System Integration andTesting

All the different units explained above where put together such that the fingerprint scanner, camera and smart cart reader writer for the registration was added to the registration platform running on a Windows system. The registration platform was also connected to the online Server.

The result website was hosted online at [E-voting Result\(https://bit.ly/32Y5z6q\)](https://bit.ly/32Y5z6q) and linked to the onlineServer.

The administrator dashboard was installed on a Windows system and linked to the online Server as well.

At the voting device end, the fingerprint module is coupled to the Arduinouno, also the smart card reader and LCD screen 16 * 2 width is connected to the Arduinouno and coupled into the voting system. The battery unit is added to the voting device too and the voting software is burnt to a memory card and inserted into the Arduinouno memory card slot. The system is started up and the voting device is working.

Table 4.3: Overall System Testing

Test	Steps	Expected Result	Test Result
On/Off	Power the system on and off	On power ON, The system should correctly boot-up within 20 seconds. On power OFF, the system should shut down within 10 seconds	Expected result gotten, as system started within 15 seconds and was shut down within 7 seconds.
Register a voter	Register the finger of the voter in the arduino software.	Display Registration Successful	Registration Successful displayed
Cast vote	Place the finger on the finger print sensor, if matched the system confirms the vote with fingerprint	Screen should display "Cast your vote "	"Cast your Vote" Displayed

View election result	The result with the no. of votes for each candidate should be shown on the lcd display.	Result should show	Result is shown
----------------------	---	--------------------	-----------------



Figure 4.2: Results displayed on the lcd

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

The manual system of voting has failed to tackle the basic issues necessary for a trusted voting environment which has evidently driven some of its citizens to apathy.

The E-voting system was implemented to solve the proximity bottlenecks, unnecessary time delays, with very secure and accurate recording of votes. The system has been thoroughly tested in voting accuracy, ruggedness, responsiveness, battery life expectancy, and security by means of simulation and mini voting sessions to be a successful one.

It is seen that the system is fault tolerant at all end points (registration, voting platform and the server).

The voting device can last for more than 6 hours which is very sufficient for a quick system like ours.

This system will provide boundless voter participation in remote areas with very little or no cost on the voter greatly reducing apathy. Further improvements can be done on the system to increase the credibility of the votes and further reduce proximity issues.

5.2 Recommendation

The following recommendations are made for optimal performance of the system:

1. The voting device should be operated in a dry environment with a fairly stable internet connection.

The following functionalities could be added to improve on the project:

1. Internet Voting (I-voting): the use of smart phones or any internet connected device to cast votes from any location.
2. The registered cards could be integrated into other areas of citizenship authentication and identification such as drivers' license and e-governance.

5.3 Contribution to Knowledge

Many works have been done with respect to making the electoral process better by increasing voters' interest to participate in the election and based on these existing solutions, this project model introduces the concept of voting at the closest polling unit while vote is counted where it belongs.

REFERENCES

- [1] Paul David Webb, Roger Gibbins, Heinz Eulau, "Election", Encyclopaedia Britannica. [Online]. Available: <https://www.britannica.com/topic/election-political-science>. [Accessed: Aug. 05,2019].
- [2] Toba Paul Ayeni, AdebimpeOmolayoEsan, "The Impact of ICT in the Conduct of Elections in Nigeria", American Journal of Computer Science and Information Technology, February 09, 2018 . [Online]. Available: <http://www.imedpub.com/articles/the-impact-of-ict-in-the-conduct-of-elections-in-nigeria.php?aid=22211>. [Accessed: Aug. 05,2019].
- [3] ACE, E-voting, The Electoral Knowledge Network, n.d., [Online]. Available: <http://aceproject.org/ace-en/focus/e-voting/default>. [Accessed: Aug. 07,2019].
- [4] Victor Ekwealor, Inside Nigeria's first ever electronic voting exercise in Kaduna State, TechpointAfrica, May 14, 2018, [Online]. Available: <https://techpoint.africa/2018/05/14/kaduna-electronic-voting/>. [Access: Aug. 10,2019].
- [5] Seth Rosenblatt, Jason Cipriani, Two-factor authentication: What you need to know (FAQ), CNET, June 15, 2015, [Online]. Available: <https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq>. [Accessed: Aug. 10,2019].
- [6] Alexandra Petru, What is two-factor authentication (2FA)?, iPhone Backup Extractor, Oct. 08, 2017, [Online]. Available: <http://www.iphonebackupextractor.com/blog/2016/jun/3/extract-data-two-factor-authentication/>. [Accessed: Aug. 11,2019].
- [7] vanTilborg, Henk C.A.; Jajodia, Sushil, eds. (2011). *Encyclopedia of Cryptography and Security, Volume 1*. Springer Science & Business Media.p.1305.
- [8] Jason Cipriani, Seth Rosenblatt, Two-factor verification: What you need to know (FAQ), CNET, June 15, 2015, [Online]. Available: <https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq>. [Accessed: Aug. 10,2019].

- [9] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi “On the (In) Security of Mobile Two-Factor Authentication” Lecture Notes in Computer Science, pp. 365-383, Nov 2014.
- [10] AlirezaPirayeshSabzevar, AngelosStavrou “Universal Multi-Factor Authentication Using Graphical Passwords”, Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems. pp. 625-632,2008.
- [11] Olufemi Sunday Adeoye “Evaluating the Performance of two-factor authentication solution in the Banking Sector” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.
- [12] Rahul Kale, Neha Gore, Kavita, NileshJadhav, SwapnilShinde “ Review Paper on Two Factor Authentication Using Mobile Phone” International Journal of Innovative research and Studies, Vol. 2, Issue 5, pp. 164 - 170, May2013.
- [13] vanTilborg,HenkC.A.;Jajodia,Sushil,eds.(2011).*EncyclopediaofCryptographyandSecurity, Volume 1*. Springer Science & Business Media.p.1305.
- [14] CardLogix Corporation, Smart Card Basics, CardLogix Corporation, 2010. [Online] Available from: <http://www.smartcardbasics.com> [Accessed1/05/19].
- [15] TarunAgarwal, How does the Smart Card Works?,ElProCus, n.d. [Online] Available from: <https://www.elprocus.com/working-of-smart-card/> [Accessed 1/05/19].
- [16] MichaLBairanzade, Smart card integration and specifications, ASPENCORE, 2002. [Online] Available from:https://www.eetimes.com/document.asp?doc_id=1200923 [Accessed1/05/19].
- [17] Wikipedia, Smart card, Wikipedia, Wikipedia, n.d. [Online] Available from: https://en.wikipedia.org/wiki/Smart_card [Accessed 29/04/19].
- [18] D. Maio, and D. Maltoni, “Direct gray-scale minutiae detection in fingerprints”, IEEE

Transactions Pattern Analysis and Machine Intelligence, vol. 19(1), pp. 27-40,199.

Biometric based Electronic Voting Machine using Arduino Microcontroller and Fingerprint sensor

by hemanth I

Submission date: 16-Apr-2021 11:45PM (UTC+0700)

Submission ID: 1561107011

File name: plagiarismreport-converted11.pdf (1,017.53K)

Word count: 12027

Character count: 70621

Biometric based Electronic Voting Machine using Arduino Microcontroller and Fingerprint sensor

⁸ Submitted in partial fulfillment of the requirements for the award of Bachelor of
Engineering Degree in Electronics and Communication Engineering

by
Lakkimsetti Hemanth(37130216)
Madala Adithya(37130224)



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS
ENGINEERING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY (DEEMED TO BE
UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

MARCH 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

www.sathyabama.ac.in



**DEPARTMENT OF ELECTRONICS AND
COMMUNICATION ENGINEERING
BONAFIDE CERTIFICATE**

This is to certify that this Project Report is the bonafide work of **Lakkimsetti Hemanth(37130216) and Madala Adithya(37130224)** who carried out the project entitled **“BIOMETRIC BASED ELECTRONIC VOTING MACHINE USING ARDUINO MICROCONTROLLER AND FINGERPRINT SENSOR”** under our supervision from September 2020 to March 2021.

Internal Guide

Dr. G.D. Anbarasi Jebaselvi, M.E.Ph.D

Associate Professor, Department of ECE

Head of the Department

Dr. T. RAVI, M.E.,

Ph.D.

Submitted for Viva voce examination held on _____

Internal Examiner

External Examiner

DECLARATION

We, **Lakkimsetti Hemanth(37130216)** and **Madala Adithya(37130224)** hereby declare that the Project Report entitled “**BIOMETRIC BASED ELECTRONIC VOTING MACHINE USING ARDUINO MICROCONTROLLER AND FINGERPRINT SENSOR**” done by us under the guidance of **Dr. G.D. Anbarasi Jebaselvi,M.E.Ph.** Dis submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

1)

2)

DATE:

PLACE: **SIGNATURE OF THE CANDIDATES**

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr. N.M.NANDHITHA, M.E., Ph.D. Dean, School of Electrical and Electronics Engineering** and **Dr. T. RAVI, M.E., Ph.D. Head of the Department, Department of Electronics and Communication Engineering** for providing us necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Dr. G.D.Anbarasi Jebaselvi, M.E.Ph.D** Associate Professor, Department of ECE for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of the project work.

We wish to express our thanks to all teaching and Non-teaching staff members of the **Department of Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

We express our gratitude to our parents for their constant encouragement and support for the completion of the project.

ABSTRACT

Fundamental right to vote or simply voting in elections forms the basis of democracy. One of the key yardsticks used to measure a state's democratic status is the conduct of frequent, competitive, participatory, credible, and nonviolent elections. Since we began practising democracy, elections have been conducted using the manual method of voting, but these elections have been marred by numerous electoral malpractices and glitches. Aggressive attacks on voters, outcome manipulations, vote buying, and the remoteness of polling centres are only a few examples. There are sufficient reasons to justify the creation and implementation of an electronic voting system that addresses the majority of these issues. The e-voting system aims to eliminate the bottlenecks evident in the manual voting system such as the lengthy registration process, unnecessary transportation, election violence and ultimately the incredibility of the votes.

This was accomplished by creating a time-saving registration platform that instantly registers a voter and issues them a voter card. The voter can also vote at their nearest, secure, and convenient polling station, and their votes will be counted correctly.

In comparison to the manual method, the results of subsequent tests were very impressive in terms of time, security, and accuracy.

Such a system, with all of these capabilities, will go a long way toward alleviating the aforementioned issues with the electoral process's current manual voting system.

Table of Contents

CHAPTER No.	TITLE	PG.NO
1	INTRODUCTION	11
1.1	Background of Study	11
1.2	Electronic-voting System Overview	11
1.3	Problem Statement	12
1.4	Aim and Objectives	12
1.5	Significance of the Project	13
1.6	Scope/Limitations of the Work	14
1.7	Project Outline	14
2	LITERATURE REVIEW	16
2.1	Theories of the Technologies Involved	16
2.1.1	Overview of Two-factor Authentication	16
2.1.2	Smart Card Technologies	19
2.1.3	Fingerprint Scanner	22
2.1.4	Database Technologies	27
2.2	Summary of the Reviewed Literature	33
3	METHODOLOGY AND SYSTEM DESIGN	35
3.1	Methodology	35
3.2	Research Purpose	35
3.3	Research Approach	35
3.4	Research Conclusion	35
3.5	Result Interface	37
3.6	Specifications	38
3.6.1	16* 2 width LCD Screen	38
3.6.2	Finger print Scanner	38
3.6.3	Arduino UNO	39
4	SYSTEM IMPLEMENTATION AND ANALYSIS	40
4.1	Voting Interface	40
4.2	System Integration and Testing	42

¹
5 CONCLUSION AND RECOMMENDATION 45

5.1 Conclusion 45

5.2 Recommendation 45

5.3 Contribution to knowledge¹ 45

6 REFERENCES 46-47


LIST OF TABLES

Table 3.1: Recommended LCD Screen 16 * 2 width Specification	10	38
Table 3.2: Recommended Fingerprint Scanner Specification	2	38
Table 4.1: Unit test for the LCD screen	6	41
Table 4.2: Unit test for the Fingerprint Scanner	2	42
Table 4.3: Overall System Testing		43
		61

LIST OF FIGURES

Figure 2.1: RSA SecurID token, an example of a disconnected token generator	18
Figure 2.2: A Pictorial representation of a Smart Card System	19
Figure 2.3: ISO-7816 standard pin-out of a basic Smart card chip	20
Figure 2.8: A Fingerprint Scanner	22
Figure 2.9: Block Diagram of a Fingerprint System	23
Figure 2.10: Components of the Database Environment	28
Figure 3.1: System Functional Flowchart	36
Figure 3.2: The Result Interface Flowchart	37
Figure 3.3: LCD Display	38
Figure 3.4: Finger Print Display	39
Figure 3.5: The arduino microcontroller	39
Figure 4.1: The Voting Interface Implementation	40
Figure 4.2: Results Displayed on the lcd screen	44

LIST OF ABBREVIATIONS

EVS	-	Electronic VotingSystem
INEC-		Independent National ElectoralCommission
ICT	-	Information CommunicationTechnology
BEME-		Bill of Engineering Measurement andEvaluation
2FA	-	Two-FactorAuthentication
ATM-		Automated TellerMachine
PIN	-	Personal IdentificationNumber
OTP	-	One TimePassword
GPS	-	Global PositioningSystem
USB	-	Universal SerialBus
PDA	-	Personal DigitalAssistant
ISO	-	International StandardOrganization
IEC	-	International Electrical Community
RFID-		Radio Frequency Identification EMV
-		Europay, MasterCard, Visa
APDU-		Application Protocol DataUnit
IAFIS-		Integrated Automated Fingerprint IdentificationSystem
CASE-		Computer-Aided SoftwareEngineering
DBMS-		Database ManagementSystem
SQL	-	Structured Query Language
PVC	-	Permanent VotersCard
ATM-		Automated TellerMachine

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Decisions must be taken between multiple choices in every democratic setting with people with varying and inconsistent opinions. This occurs in the corporate world, the educational world, social organisations, and, most notably, in government. Voting is one of the methods for making such a decision. Voting is a formal mechanism for individuals to show their support or opposition to a motion. This method is often used in the governance field of many organisations to appoint or nominate a chief. Elections are one of the most important fields where voting is used. The formal process of nominating a candidate for public office or endorsing or refusing a political proposal is known as an election..[1]

1.2 Electronic-voting System Overview

E-voting (Electronic Voting) as a term encompasses a broad range of voting systems that apply electronic elements in one or more steps of the electoral cycle [3]. In a broad sense, e-voting can take many forms, including e-collection, e-verification, internet voting, remote online voting, and so on. An e-voting system is any system that can provide both electronic and online voting, according to the concept of a system as something that takes an input and produces an output. E-registration, e-verification, e-collation, remote online voting, and real-time result display may all be included. For an E-voting system (EVS) to work properly, it must have the following components.:

- ❑ An interactive voting user interface on an electronic device which provides a friendly environment for voters to authenticate and cast their votes, it also serves as a means of collection the individual votes and storing them in the local and central database.
- ❑ An administrative dashboard for voters registration, details update and elections coordination and monitoring.
- ❑ A database management system for the storage of election, voting and voters data.
- ❑ A result display interface.

E-voting systems reduce overall election costs and increase voter participation by providing voters with a simple and convenient way to vote. Most importantly, they address the issue of voters travelling long distances to a specific location for their votes to be counted, as well as ballot box snatching, which is common in the United States.

The election process has seen significant technological advancements, especially in the areas of result collation and transmission. Owing to a lack of legislative basis, the Independent National Electoral Commission INEC has not completely incorporated the use of technology for collation [2]. However, ICT is used in most elections around the world to some extent, at least to summarise and aggregate votes. This electronic adaptation is the culmination of a long period of evolution during which not only the processes for casting votes, but also the technical means for doing so, have evolved significantly.

1.3 Problem Statement

The present voting system applicable in the electoral system has proved inefficient as the voters' registration process is slow, the manual collation of results takes time and gives room for result manipulation, also the inaccessible nature of election venues which includes the long distances to be covered by voters' to their registered location increases. The issues of ballot box snatching and destruction, as well as other election violence and issues associated with conventional ballot paper voting, all taint the intent of voting in an election process as a structured process of expressing individual opinions for or against a motion.

1.4 Aim and Objectives

In the quest to design a successful system to tackle the issues stated in the problem statementThe project's goal and goals are outlined below.

Aim

The aim of this project is to develop and implement a low-cost, real-time automated electronic voting system.

Objectives

Project Objectives includes

1. A detailed study of the election processes as it pertains to voting.
2. Design and develop election voting system that verifies the identity of the voters by their biometric data.
3. Design and develop an electronic device that incorporates fingerprints technology for voters accreditation, authentication and verification.
4. Design and develop an administration dashboard for the election administrators.
5. Run simulations and compare the results of the designed e-voting system

1.5 Significance of the Project

The project's benefits are itemised as follows, in light of the rapid growth of computer technology in

practically all fields of activity and its application in relation to knowledge management:

To the University

An e-voting system is beneficial to the university as:

1. It will provide a means to conduct a more or less stressful and fair elections at different levels (faculty, departments, school wide etc) in the university.
2. It will offer an in-depth knowledge of the practical approach to ICT education.
3. It will serve as a hands-on application of theories taught in class as it relates to database, software and hardware development.
4. Student and staff information can be conveniently obtained for quick access and tracking since the database is built on a versatile database management framework.
5. Its smart card system can also be applied to other fields (e.g. networking) for easy access of each individual's data.
6. It will serve as a base for other works in the field of ICT governance.

To the Society

The significance of an e-voting system to the society are itemized as follows:

1. It will provide INEC (Independent National Electoral Commission) with a means to conduct less costly and fair elections.
2. The secure and flexible system safeguards data and information to account for credible elections.
3. It will serve to reduce the workload in the process of conducting an election.
4. As it incorporates remote voting individuals can vote from their convenience.
5. It will enable INEC reduce the time wasted in collating and announcing election results.
6. It will greatly reduce and eliminate disenfranchising electorates.
7. It will serve to eliminate invalid votes, curb election violence as votes are counted immediately as they are cast.

1.6 Scope/Limitations of the Work

This project's main goal is to encourage the Independent National Electoral Commission to use electronic devices to collect voter information and allow voters to cast votes more easily and comfortably, resulting in a more reliable, successful, and cost-effective election.. The dynamic nature of the elections application interface and database structure allows for different organizations set up and conduct basic elections too. It's online interface enables real-time election monitoring and result collation. Some of its major limitations are:

1. It requires network access: Since the collection and sending of votes to the database requires an internet access which may not be readily available in some urban area would seem a limiting factor, though the local database and the printed vote can be used for counting until network is restored.
2. Setting up an e-voting system is expensive: Due to the fragile nature of such a system and the fact that its major components are currently not available locally, it will be very costly to set up, but its usage and maintenance costs are much lower than the current ballot paper system.
3. It depends on electricity to a point: In as much as it has an in built battery that can last for the required election duration on daily basis, a case of low battery would require it to recharge, which may not be possible if there is no electric power at the moment.

1.7 Project Outline

This project work on e-voting system is made up of five chapters: introduction, literature review, methodology and system design, systems implementation and result analysis, conclusion and recommendation.

In the chapter one of this project, the introduction which briefly explains voting and elections in general, is seen. It goes on to clarify the context of an e-voting system, as well as the system's goal and goals, as well as its meaning, scope, and constraints.

The second chapter dealt with a study of previous literature and the technologies used in e-voting systems. We also looked at the various approaches to e-voting systems, their application, critique, and literature reviews, as well as the various gaps in the current literature.

The block diagram of the project work, the various methodologies used in development stages, and the different phases of the project work, which include analysis, design, microcomputer programming, display programming, testing, and fabrication, are all shown in chapter three. We extensively cover the

requirements of the project, the mathematical models used designs and software incorporated in the work.

In chapter four, we talk about the measures taken and methods used in the project's actual implementation We can see checks being run to ensure that the project is running smoothly, as well as the results and their importance. We can also see the challenges that have been faced, as well as the methods and solutions that have been used to solve them or not.

And finally, in chapter five, we conclude the work and give notable recommendations for optimal operation of the product. Also we provide suggestions for improvement, enhancement and optimization of our existing work. We also outline the major contribution to the body of knowledge in which our work has achieved.

CHAPTER 2

LITERATURE REVIEW

2.1 Theories of the Technologies Involved

2.1.1 Overview of Two-factor Authentication

Two-factor authentication (also known as 2FA) is a form of multi-factor authentication, or a subset of it. Multi-factor authentication is a type of machine authentication in which a user is granted access after successfully presenting two or more pieces of evidence (or factors) to an authentication device, such as knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is) (something the user and only the user is).

As a result, 2FA is a method of verifying users' asserted identities by combining two factors: 1) what they know, 2) something they have, or 3) what they are. Withdrawing money from an ATM is a clear example of two-factor authentication; the transaction can only be completed with the right combination of a bank smart card (something the user has) and a PIN (something the user knows). Another example is to use a one-time password (OTP) or a code created and obtained by the user (e.g. a security token) on a smartphone that only the user has access to.

Two-step verification, also known as two-step authentication, is a method of verifying a user's assumed identity by using something they know (password) and a second factor other than something they have or are. A user repeating back something that was sent to them via an out-of-band process is an example of a second phase. A six-digit number provided by another system that is shared by the user and the authentication system may also be used as the second stage.

Authentication Factors

Since an unauthorised actor is unlikely to be able to supply the factors required for entry, multiple authentication factors are used to prove one's identity. (e.g a building, or data,)

The user is then blocked despite being secured by multi-factor authentication. A multi-factor authentication scheme's authentication factors may include:

- ❑ some physical object in the possession of the user, such as a USB stick with a secret token, a bank smart card, a key, etc.
- ❑ some secret known to the user, such as a password, PIN, TAN etc.
- ❑ some physical characteristic of the user (biometric), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.
- ❑ somewhere you are, such as connection to a specific computing network or utilizing a GPS signal to identify the location.

The above authentication factors are further discussed under the following sub headings:

1. Knowledge Factors
2. Possession Factors
3. Inherent Factors
4. Location Based Factors

Knowledge Factors: are the most widely used authentication method. In order to authenticate, the user must prove knowledge of a secret in this form. A password is a hidden word or string of characters used to verify the identity of a user. This is the most widely used authentication method. Passwords are used as one aspect of authentication in many multi-factor authentication techniques. [nine] Longer personal identification numbers (passwords) and shorter, strictly numeric personal identification numbers (PINs) are widely used for ATM entry. Passwords are traditionally meant to be memorised. Many hidden questions, such as "Where were you born?" are poor examples of intelligence factors since they could be identified by a large number of people or could be studied.

Possession Factors: (defined as "something the user and only the user has") have been used for authentication in the form of a key to a lock for centuries. The basic principle is that the key encapsulates a secret that is exchanged between the lock and the key, and possession factor authentication is based on the same principle.

in terms of operating systems. A security token is an example of a possession factor. Possession factors

could be grouped as follows:

- i. Disconnectedtokens.
- ii. Connectedtokens.
- iii. Software tokens.

Disconnected tokens have no connections to the client computer. They typically use a built-in screen to display the generated authentication data, which is manually typed in by the user.[12]



Figure 2.1: RSA SecurID token, an example of a disconnected token generator

Tokens that are physically attached to the machine to be used are known as connected tokens. These devices automatically transmit data. (#13) Card readers, wireless tags, and USB tokens are all examples of various styles.[13]

A software token (also known as a soft token) is a two-factor authentication protection device that can be used to authorise access to computer services. Software tokens can be duplicated and placed on a general-purpose electronic device like a desktop computer, laptop, PDA, or cell phone. (This is in contrast to hardware tokens, which store credentials on a dedicated hardware device and therefore cannot be duplicated unless the device is physically invaded.) A soft token may or may not be a system with which the user communicates. To serve this function, an X.509v3 certificate is usually loaded onto the computer and securely stored..

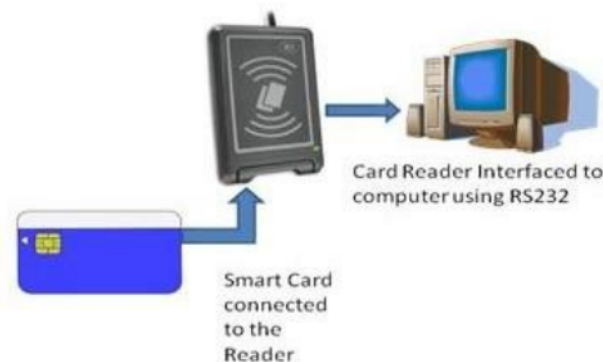
Inherent Factors: are factors associated with the user, and are usually biometric methods, including fingerprints, face, voice, or iris recognition. Behavioral biometric such as keystroke dynamics can also be used.

Location Based Factors: A fourth element, the user's physical position, is increasingly coming into play. A user could be able to authenticate using only a pin code when hardwired to the corporate network, but while off the network, a code from a soft token could be needed as well. When access to the office is regulated, this may be considered an appropriate norm. Network admission control systems operate in a similar manner, with the level of network access being determined by the network to which your computer is linked, such as WIFI vs wired connectivity. This also enables a user to switch between offices while maintaining the same degree of network access.

Authentication is a critical security feature in applications, and it can be improved with two-layer authentication to increase confidence in the system's overall integrity.

2.1.2 Smart Card Technologies

A smart card, also known as a chip card, is a plastic card with an embedded computer chip—either a memory or a microprocessor—that stores and transmits data. This information is normally associated with either a monetary value, information, or both, and is stored and processed inside the card's chip.



The information on the card is transferred using a reader that is part of a computer system.

Figure 2.2: A Pictorial representation of a Smart Card System

Smart card-enabled systems are currently in use in a variety of industries, including healthcare, banking, governance, entertainment, and transportation. Smart cards can support both of these applications by providing additional features and protection. Smart cards are a type of machine-readable card that is used for authentication. Markets that have previously been served by other machine-readable card technologies, such as bar-code and magnetic stripe, as well as traditional authentication methods, such as passwords and forms, are converting to smart cards as the measured return on investment is revisited

year after year by each card issuer. ISO/IEC is a global standard-setting organisation for technology, which includes plastic chip cards. ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693, and ISO/IEC 7501 are the most common smart card standards. The physical dimensions, electrical interface, communication protocols, and database structure approach are all described by these principles. A smart card system is made up of two parts: the smart card and the card reader.

Figure 2.3: Standard pin-out of a simple Smart card chip according to ISO-7816.



The Smart CardChip

To bear the electronic chip, the smart card uses the same basic plastic media as magnetic stripe-based cards: To bind the silicon to the outside world, eight gold-plated contacts are used.. As shown in figure 2.3, these contacts are arranged according to the ISO7816-1 specification.

Description of Smart CardPin-out

1. C1 (VCC +5V DC): Input power supply (optional use by the card)
2. C2 (RESET): Reset signal, which is used to clear the card's communications.
3. C3 CLOCK : Provides the card with a clock signal, from which data communications timing is derived
4. C4 (RESERVED AUX1): Optionally used for USB interfaces and other uses.

5. C5 (GND): Ground (reference voltage)
6. C6 (Vpp): Voltage input programming (optional). This touch can be used to provide the voltage needed to programme or delete the non-volatile memory within the device. This was designated as a programming voltage in ISO/IEC 7816-3:1997: an input for a higher voltage to programme permanent memory (e.g., EEPROM). It is designated as SPU in ISO/IEC 7816-3:2006 for regular or proprietary use as input and/or output..
7. C7 (I/O) : Input or Output for serial data (half-duplex) to the integrated circuit inside the card.
8. C8 (RESERVED AUX2): Optionally used for USB interfaces and other uses.

Advantages of SmartCards

1. Smart cards can have a higher degree of protection than magnetic stripe cards since they contain microprocessors that can process data without the need for external connections.
2. Smart cards are typically made of plastic, generally polyvinyl chloride and are of dimension 85.60 by 53.98 millimeters, which makes them portable and very easy to carry about.
3. Another advantage of smart cards is that once information is stored on a smart card, it can't easily be deleted, erased or altered. As such, smart cards are good for storing valuable data that can't be -- or shouldn't be -- easily reproduced.
4. Smart card technology is generally safe against electronic interference and magnetic fields, unlike magnetic stripe cards. In addition, applications and data on a card can be updated through secure channels so issuers do not necessarily have to issue new cards when an update is necessary.
5. Multi-service smart card systems can enable users to access more than one different service with just one smartcard.
6. The cost a smart card is very affordable and it is not costly to implement and manage.

Disadvantages of SmartCards

1. While smart cards have many advantages, the cards themselves -- as well as the smart card readers -- can be expensive as it is not locally sourced in at the moment.
2. Another drawback to smart cards is that not all smart card readers work for all smart card forms. Some smart cards and readers use proprietary software that is incompatible with other readers, and

some smart cards and readers use nonstandard protocols for data storage and card interface.

3. Although smart cards are more secure in many applications, they are still susceptible to certain attacks. Smart card technology is vulnerable to attacks that can retrieve information from the chip. The on-chip private key used by public key algorithms can be deduced using differential power analysis. Some symmetric cypher implementations are also vulnerable to timing attacks and differential power analysis.
4. Smart cards may also be physically disassembled in order to gain access to the on-board microchip.

The automatic method of verifying a match between two human fingerprints is known as fingerprint recognition or fingerprint authentication. An ink-less scanner is usually used to obtain a better print impression. In terms of ridge bifurcations and ridge endings, the digital image of the fingerprint contains many special features known as minutia [19].

2.1.3 FingerprintScanner

A fingerprint scanner is a computer that captures a digital image of a person's fingerprint pattern. The comparison of several features of the print pattern is usually needed when analysing fingerprints for matching purposes. Patterns, which are ridge aggregate characteristics, and minutia points, which are unique features found within patterns, are examples.



Figure 2.8: A Fingerprint Scanner

Parts of a FingerprintScanner

The fingerprint scanner consists of fingerprint sensor, ADC (Analog to Digital Converter), flash ROM

and DSP (Digital Signal Processing) chip.

1. Fingerprint Sensor: The fingerprint sensor is used for scanning the finger impression. The scanning data is in the form of analog. Further, this process is converted by the A/D converter.
2. A/D Converter: Here the analogue data from the sensor is converted to the digital data and it is transferred to the processor.
3. Flash ROM: The flash ROM is used to store the data temporarily in the DSP processor and this will work until the data is transferred to the main memory of the host.
4. DSP Chip: The DSP chip is used for processing and receiving the data. For further transfer of data the DSP port is used.
5. DSP Port: It is used for the communication between DSP processor and memory (database).

Components of a Fingerprint System

A typical fingerprint system consists of four major components, which consist of:

1. Image capture
2. Feature extraction
3. Pattern matching
4. Database

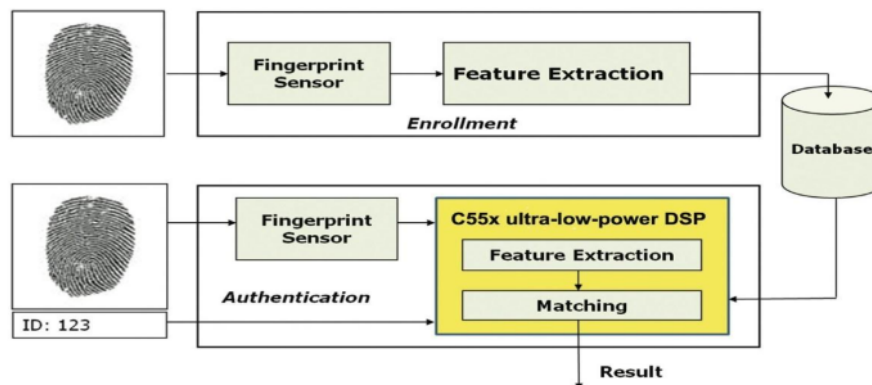


Figure 2.9: Block Diagram of a Fingerprint System [20].

Fingerprint systems convert illuminated fingerprint images into digital code, which is then used by other

software for enrollment (fingerprint registration) and verification (authentication or verification of registered users). The scanner captures high contrast, high resolution fingerprint images that are practically distortion-free using an advanced CMOS image sensor. A series of sophisticated algorithms extract data from the image, mapping the fingerprint's distinguishing characteristics.

This information is then translated into a digital template, which is an encoded binary string that is saved in a database. The fingerprint picture itself is never saved. A patented matching algorithm compares the new prototype made from the extracted characteristics from the input fingerprint on the optical module to a previously stored sample to recognise or validate a fingerprint. It takes about a second for the entire matching process to complete. Depending on the system setup, authentication takes place locally on the client or remotely on a server. [20].

Mode of Operation of a FingerprintSystem

A fingerprint biometric system can operate in two modes:

Verification mode: The system performs a one-to-one (1:1) comparison of a captured fingerprint with a specific template stored in the database in order to verify the individual is the person they claim to be.

1. Identification mode: The system performs a one-to-many (1:N) comparison against fingerprints in the database in an attempt to establish the identity of an unknown individual.

Applications of Fingerprint BiometricTechnologies

There are numerous applications for the use of Biometric Technology, but the most common ones are as follows:

1. Logical Access Control: This refers to gaining access to a computer network either at the place of the business or corporation or via a secured remote connection from a distant location. Fingerprint systems are deployed to allow for easy access for authenticated users.
2. Physical Access Control: refers to giving a person or an employee of a business or a corporation access to a secure building, or even a secure office from within it. Fingerprint systems are installed at entrance points to grant entrance access to only authentic employers or person with such access or clearance.
3. Time and Attendance: Here, fingerprint biometric is used to take records of attendance of the members of an organisation. The time of arrival and departure can also be recorded and stored in

a database for reference purposes.

4. Law Enforcement: This is the most widely known application of fingerprint biometric technologies. Here law enforcement agencies implement fingerprint biometric system as a means of collecting identities of criminals. IAFIS (Integrated Automated Fingerprint Identification System), a worldwide database of fingerprints of criminals is an example of such. IAFIS administrated and maintained by the FBI (Federal Bureau of Investigation) in the United States[21].
5. Surveillance: This is simply keeping tabs of a large group of people, and from there, determining any abnormal behavior from an established baseline. Fingerprint systems are deployed also with face recognition to track for example people with criminal records any erratic behavior.

Advantages of Fingerprints Technologies

1. Fairly small storage space is required for the biometric template, reducing the size of the database required.
2. It is one of the most developed biometrics.
3. Each and every fingerprint including all fingers are unique, even identical twins have different fingerprints and as such it is a safe way of identifying individuals.
4. Sound potential for forensic use as most of the countries have existing fingerprint databases.
5. Relatively inexpensive and offers high levels of accuracy.

Disadvantages of Fingerprints Technologies

1. Even with its many benefits, fingerprint systems are also associated with some disadvantages that makes their implementation controversial, and they includes:
2. The fingerprint scanner does not take into consideration when a person physically changes. Changes such as growth tends to change fingerprints and accidents such as bruises or cuts or even dirt on the finger can make an already existing user's verification invalid as the fingerprint is now altered.
3. For some people it is very intrusive, because is still related to criminal identification.
4. If anyone can access to an authorized user's prints, he can trick the scanner. The criminal can cut off somebody's finger to get a scanner security system but some scanners have additional pulse and heat sensors to verify that the finger is alive, but these systems can still be fooled by a gelatin print mold over a real finger[22].
5. Having a high security system may require expensive computer hardware and software, certain fingerprint scanners can be quite expensive.

Fingerprint authentication is the cheapest, fastest, most convenient and most reliable way to identify a particular person. It has many functional advantages over traditional systems such as passwords. The greatest strength of the fingerprint authentication technology, is the fact that the fingerprint does not change over time.

Today, fingerprint recognition technology is used for mostly security and identification purpose. As

fingerprint recognition technology advances, more affordable and compact fingerprint recognition devices are expected to become available, and fingerprint recognition will be regarded as a safe and convenient authentication method.

2.1.4 Database Technologies

At the heart of every fully designed system are the collection, storage, aggregation, manipulation, dissemination, and management of data [23]. **Data** are raw facts. The word raw indicates that the facts have not yet been processed to reveal their meaning. **Information** are data that have been processed in such a way that the knowledge of the person who uses the data is increased. These facts are made available for processing because they are stored at a place for future reference. The two main techniques for data storage in computers are: file system and database.

A file system is a method of storing and organising computer files and the data they contain in such a way that they are easy to locate and access. File systems use a storage unit such as a hard disc or CD-ROM to keep track of where the files are physically located. A file system can be used to store less complex data, but storing an organization's data, such as employee information, financial records, and so on, requires a well-structured system, which is referred to as a database.

Database is as an organized collection of logically related data. It is a collection of data, typically describing the activities of one or more related organizations. A database can also be seen as a shared, integrated computer structure that stores a collection of:

- ⑦ End-user data, that is, raw facts of interest to the enduser.
- ⑦ Metadata, or data about data [23], through which the end-user data are integrated and managed.

The file systems became obsolete as their integration and use becomes difficult when the volume of data stored increases. Its numerous disadvantages led to the development of database as an easier means for data storage, but as the need for a good data manipulation system increased, there was need to develop a management system for databases for quick access and control and that gave rise to the Database Management System (DBMS).

Components of the Database Environment

The database operational environment shown in Figure 2.10 is an integrated system of hardware, software, and people, designed to facilitate the storage, retrieval, and control of the information resource and to improve the productivity of the organization. They are includes:

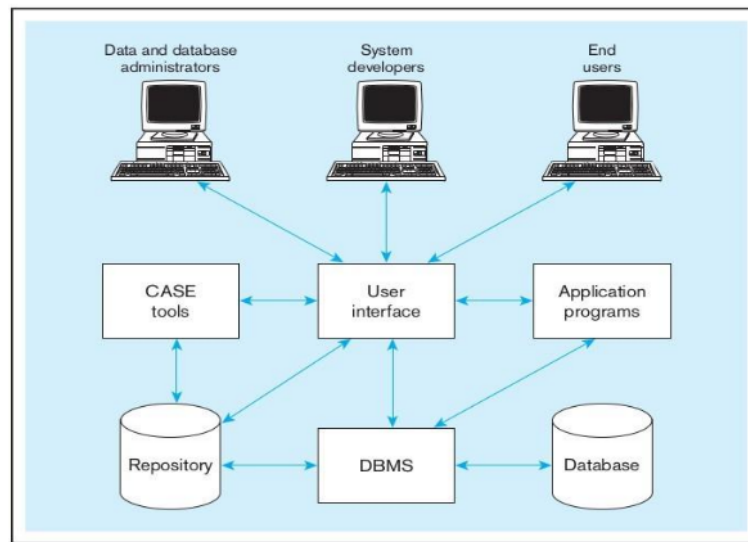


Figure 2.10: Components of the Database Environment [24].

Computer-aided software engineering (CASE) tools: CASE tools are automated tools used to design databases and application programs.

Repository: A repository is a set of metadata that is useful for maintaining databases and other information system components.

DBMS: It's a software framework for creating, maintaining, and controlling access to user databases.

Database: It is a logically linked set of data that is structured to satisfy the information needs of different users in an organisation. It's important to understand the difference between a database and a repository. Data descriptions are stored in the archive, while data events are stored in the database.

Application programs: The database is created, maintained, and information is provided to users using computer-based application programmes.

User interface: This includes languages, menus, and other facilities by which users interact with various system components, such as CASE tools, application programs, the THINGSPEAK DATABASE, and the repository.

Data and database administrators: Data administrators are tasked with overseeing the management of an organization's data resources. Database managers are in charge of the physical design of databases as well as the management of technical problems in the database system.

System developers: They are people who develop new application programmes, such as systems analysts and programmers. CASE techniques are often used by system developers for system requirements analysis and software design.

End users: These are the people who add, remove, and change data in the database, as well as those who request or obtain information from it. The THINGSSPEAK DATABASE must handle all user interactions with the database..

Database ManagementSystem

A database management system (DBMS) is a piece of software that allows you to use a database. The primary goal of a THINGSSPEAK DATABASE is to provide a standardised method for generating, modifying, storing, and extracting data from a database. It allows end users and application programmers to exchange data and to share data across different applications rather than propagating and storing data in new files for each new application [24]. Controlling data access, enforcing data integrity, managing concurrency control, and restoring a database are all possible with a THINGSSPEAK DATABASE.

There are many terms associated with the THINGSSPEAK DATABASE used to explain the different operations in a database environment, they includes terms like query -- a specific request issued to the THINGSSPEAK DATABASE for data manipulation — for example, to read or update the data. Simply put, a query is a question.

The terms database and THINGSSPEAK DATABASE are most times used interchangeably to refer to the database technology and as such we adopt such use here to us focus on the technological aspects of the database approach.

Advantages ofDatabase

As a database is only as useful as its THINGSSPEAK DATABASE , the advantages of a THINGSSPEAK DATABASE are as follows:

1. Improved data sharing: The THINGSSPEAK DATABASE helps create an environment in which end users have better access to more and better-managed data. Such access makes it possible for end users to respond quickly to changes in their environment.
2. Improved data security: The more users access the data, the greater the risks of data security breaches. Corporations invest considerable amounts of time, effort, and money to ensure that corporate data are used properly. A THINGSSPEAK DATABASE provides a framework for

better enforcement of data privacy and security policies.

3. Better data integration: Wider access to well-managed data promotes an integrated view of the organization's operations and a clearer view of the big picture. It becomes much easier to see how actions in one segment of the organisation affect other segments.
4. Minimized data inconsistency: Data inconsistency exists when different versions of the same data appear in different places. For example, data inconsistency exists when a company's sales department stores a sales representative's name as "MaryBlessing" and the company's personnel department stores that same person's name as "Mary-Blessing C.," or when the company's regional sales office shows the price of a product as #4,500 and its national sales office shows the same product's price as #4,490. The probability of data inconsistency is greatly reduced in a properly designed database.
5. Improved data access: The THINGSSPEAK DATABASE makes it possible to produce quick answers to ad hoc queries
 - a spur-of-the-moment question [23]. The THINGSSPEAK DATABASE sends back an answer (called the query result set) to the application. For example, end users, when dealing with elections data, might want quick answers to questions (ad hoc queries) such as:
 - ❑ What was the total number of registered voters during the past six months?
 - ❑ What is the total number of students who can vote?
 - ❑ How many candidates are contesting for a particular election?
6. Improved decision making. Better-managed data and improved data access make it possible to generate better-quality information, on which better decisions are based. The quality of the underlying data determines the quality of the information produced. Data quality refers to a holistic approach to ensuring data accuracy, validity, and timeliness. While the THINGSSPEAK DATABASE does not guarantee data consistency, it does provide a forum for data quality measures to be implemented.
7. A boost in end-user efficiency. End users can make fast, informed decisions based on the availability of data and the tools that turn data into usable knowledge, which can mean the difference between success and failure in the global economy.
8. Greater data independence: Application systems should be as unaffected by data representation and storage information as possible. To protect application code from such information, the THINGSSPEAK DATABASE may provide an abstract view of the data.

Disadvantages of Database

The database approach entails some additional costs and risks that must be recognized and managed when it is implemented.

1. 1. Need for new, specialised personnel: Companies that follow the database approach often need to recruit or train people to develop and implement databases, provide database management services, and manage a team of new people.
2. 2. Installation and management cost and complexity: Installing such a system may also require upgrades to the hardware and data communications systems in the organization. Substantial training is normally required on an ongoing basis to keep up with new releases and upgrades. Additional or more sophisticated and costly database software may be needed to provide security and to ensure proper concurrent updating of shared data.
3. 3. Costs of conversion: The cost of converting these older systems to modern database technology, measured in terms of resources, time, and organisational effort, can be prohibitive for a company.
4. 4. The need for explicit backup and recovery: This necessitates the creation and implementation of robust protocols for providing data backup copies and restoring databases when damage occurs.
5. 5. Organizational conflict: Disputes over data definitions, data formats and coding, rights to update shared data, and related issues are common and difficult to address, according to experience.

Types of Database

Depending upon the usage requirements, there are following types of databases available:

1. Centralized database: Information (data) is stored in a centralised location and can be accessed by users from various locations. This database form includes application procedures that enable users to access data from a remote location. End users are verified and validated using a variety of authentication procedures, and application procedures include a registration number that is used to keep track of and monitor data use.
2. Distributed database: The data is spread through many locations within an entity. These sites are linked together by communication connections, allowing them to easily access the distributed data. Homogeneous and heterogeneous distributed databases are the two types of distributed databases. Homogeneous DDBs are databases that have the same underlying hardware, run on the same operating systems, and use the same application procedures. Whereas, at different sites

of a DDB, the operating systems, underlying hardware, and application procedures may be different, which is known as heterogeneousDDB.

3. Personal database: Data is collected and stored on portable, easy-to-manage personal computers. The data is usually only viewed by a select number of people and is used by the same department of an organisation.
4. End-user database: The end user is normally unconcerned with the transactions or operations carried out at different levels, and is only concerned with the product, which may be software or an application. As a result, much like various levels'managers, this is a shared database that is explicitly developed for the end user. This database contains a summary of all facts.
5. Commercial database: These are the paid versions of large databases created specifically for people seeking information for assistance. These databases are subject-specific, and no one can afford to have such a large amount of data on hand. Commerciallinks are used to gain access to such databases.
6. 6. NoSQL database: This type of database is used to store vast amounts of distributed data. Some big data performance problems are effectively solved by relational databases; however, NoSQL databases can easily handle such issues. They are very effective at processing vast amounts of unstructured data that could be stored on several cloud virtual servers. MongoDB is an example of a NoSQL database. [25].
7. 7. Operational database: This database stores information about an organization's activities. Such databases are needed by functional lines such as marketing, employee relations, and customer service, among others.
8. 8. Relational database: These databases are divided into categories by a collection of tables in which data is classified. The table is made up of rows and columns, with each column containing data for a specific category and each row containing an instance of that data identified by the category. The Structured Query Language (SQL) is a relational database's standard user and application software interface.

There are a number of basic operations that can be performed on a table, making it simpler to expand these databases, join two databases with a similar reference, and change all existing applications.

9. Cloud database: Data is increasingly being processed in databases, also known as virtual environments, whether in a hybrid cloud, public cloud, or private cloud. A cloud database is one

that has been optimised or developed specifically for use in a virtualized environment. A cloud database has many advantages, including the ability to pay for computing space and bandwidth on a per-user basis, as well as scalability on demand and high availability.

A cloud database also gives enterprises the opportunity to support business applications in a software-as-a-service deployment.

10. 10. Object-oriented database: An object-oriented database is a combination of relational databases and object-oriented programming. While there are some items generated with object-oriented programming languages such as C++ and Java that can be stored in relational databases, object-oriented databases are better suited for those items.

Objects, rather than behaviour, and data, rather than logic, are the building blocks of an object-oriented database. A multimedia record in a relational database, for example, may be a definable data object rather than an alphanumeric attribute.

11. Graph database: The graph is made up of nodes and edges, with each node representing an individual and each edge describing the relationship between them. A graph-oriented database, also known as a graph database, is a type of NoSQL database that stores, maps, and queries relationships using graph theory. The main purpose of graph databases is to analyse interconnections. Companies may, for example, use a graph database to mine data from social media to learn more about their customers.

2.2 Summary of the Reviewed Literature

The e-voting systems we reviewed above were all developed out of a quest to enhance the voting systems to meet the recent technological frame and as well provide a means to uphold a credible election. The different e-voting systems have different levels of adoption of technology in them as seen fit by the authors and the users.

Some e-voting systems use a single device with different authentication technology, while some implement two or more devices for authentication and vote casting purposes. Based on the technology available and the interest of the users, an e-voting device that works well is developed and there is always room for constant upgrade and development as technology advances.

The common criticism about the e-voting system is the issue of software security [32], and this has posed a serious threat to the adoption of an e-voting system. In the quest to add a physical assurance to

the e-voting systems, the VVPAT (Voter Verifiable Paper Audit Trail) was advocated to be adopted to allow for manual counting of votes also at the end of the election.

LiteratureGaps

The concept of e-voting systems has its focus on eliminating the issues of multiple voting and other election malpractice associated with the conventional ballot paper voting. Though many works have been done on the area of e-voting and many countries has adopted it for different levels of election, none of them was designed to completely captured the election process. The solution to the issues of voters traveling from one location to another where their vote would count on the Federal level elections is one missing puzzle to the existing e-votingsystems.

CHAPTER 3

METHODOLOGY AND SYSTEM DESIGN

3.1 Methodology

Methodology is the systematic, theoretical analysis of the methods applied to a field of study. The aim of this chapter is to give an introduction about the general research methodology and waterfall methodology for development used in this project.

3.2 Research purpose

In the information age, it seems that the use of information technology is an unavoidable trend for the evolution of organisations in the twenty-first century, whether public or private. Electronic democracy, which is governance-oriented, and e-government, which is service-oriented, are two examples of information technology's application in public affairs. E-voting, as a critical component of e-Government systems, would inevitably contribute to the use of information technology to increase the performance of the public sector and citizen engagement through electronic forums.

The purpose of this research is to identify the factors affecting the election process and ways they can be eliminated.

3.3 Research approach

There are two main research approaches used in scientific work, quantitative and qualitative. The main difference between these two is that the aim of quantitative research is to find explanation to a phenomenon or a situation that can be generalized to other people and places while in qualitative research the aim is to gain deeper understanding of a phenomena or a situation.

Quantitative approach will be used to discover the issues that threatens the election as it relates to voters. We are making use of existing data already collected by previous literature on elections to analyze the election process and derive a conclusion on how to eliminate the issues.

3.4 Research conclusion

Based on the reviewed data collected on previous conducted elections, the main issue with the election was the issue of voters apathy towards the electoral system which is as result of

many factor such as inaccessible registration and voting venue, election violence that could lead to loss of lives, result manipulation and so on.

A system that serves to increase voters participation in the electoral process is the remedy to these issues at hand.

E-voting system serves to provide a remedy for the inaccessible registration and voting venue as eligible citizens can be registered and vote at their place of residence for their votes to count for their particular place of origin. It also provides a means to eliminate ballot box snatching as votes are counted as they are cast. There is also less room for result manipulation because the result get updated and displayed to all as votes are beingcounted.

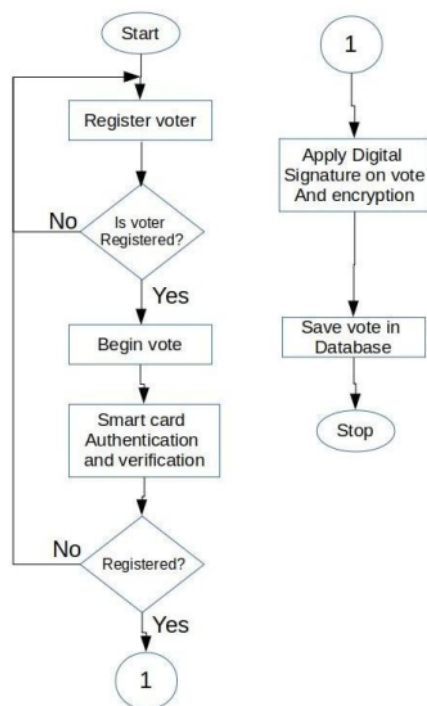


Figure 3.1: System Functional Flowchat

3.5 Result Interface

The result interface design is such that anyone can have access to election results, hence no authentication is required to access this service. Nevertheless, data is transmitted over secure protocols to insure integrity of the results being shown. The interface makes use of bar graphs and chats to show live election results. The result interface program flowchart is shown below.

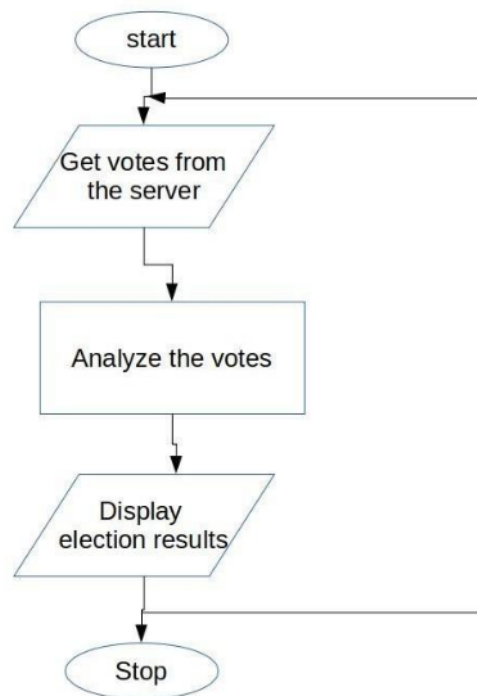


Figure 3.2: The Result Interface Flowchart

3.6 Specifications

3.6.1 16 * 2 width LCD Screen

The screen 16 * 2 width is a resistive LCD screen with a touch controller. The controller renders the graphics output of the arduino uno to the screen 16 * 2 width while sending touch responses from the screen to the arduino uno. The screen 16 * 2 width has an impressive response time and the Table

3.1: Recommended LCD Screen 16 * 2 width Specification

Property	Value
LCD size	16'' inch
Power supply	5V-12V DC
Display size	7~10 inch
Screen type	Resistance screen
LCD resolution	800*480

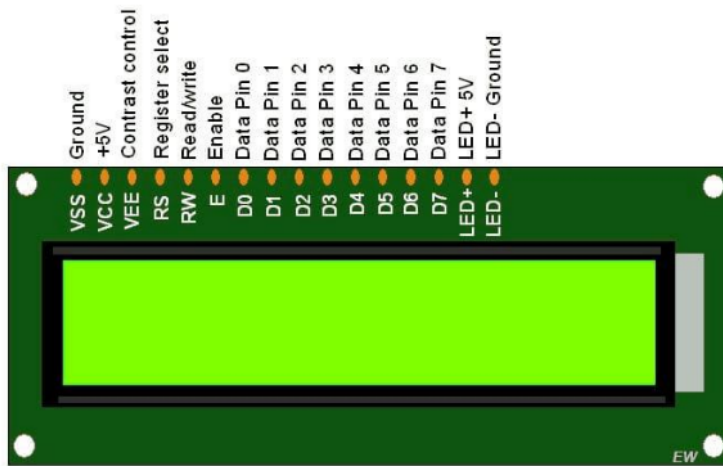


Figure 3.3: LCD Display

3.6.2 Finger print Scanner

This is one out of the two factors of authentication for the voting device, providing strong security and confidence on a voter's vote. The fingerprint scanner enables the fingerprint of the voter to be read for verification or identification of the voter.

Table 3.2: Recommended Fingerprint Scanner Specification

Property	Value
Interface	UART (TTL)

Voltage	4.2-6.0V DC
Resolution	508 DPI
Sensing area	160*160 pixel
Fingerprint capacity	200
Module Size	33.4*20.4 mm

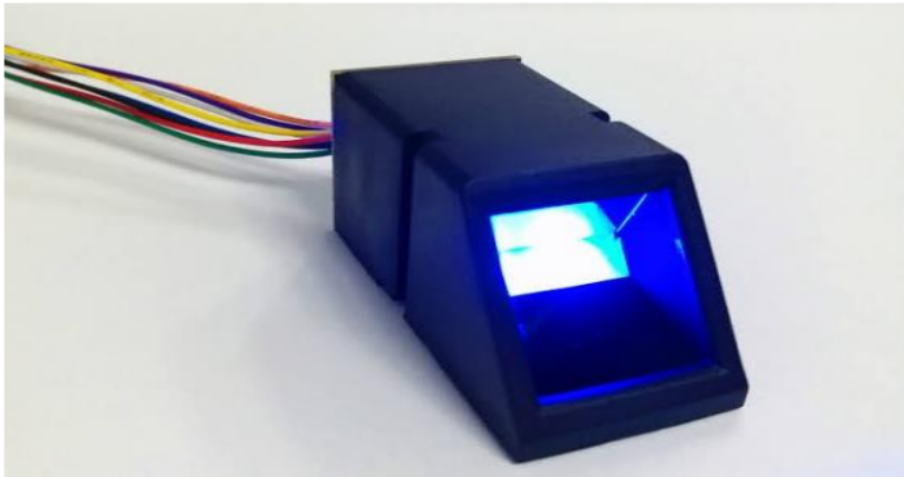


Figure 3.4: Finger print sensor

3.6.3 Arduino UNO:

The **ArduinoUno** is an open-source microcontroller board based on the Microchip ATmega32P microcontroller. The board has a number of digital and analogue input/output (I/O) pins that can be used to connect to different expansion boards (shields) and other circuits. A CPU, another Arduino/Genuino board, or other microcontrollers can all be communicated with using the Arduino/Genuino Uno.

2

Figure 3.5: The Arduino Microcontroller



CHAPTER 4

SYSTEM IMPLEMENTATION AND RESULT ANALYSIS

4.1 VotingInterface

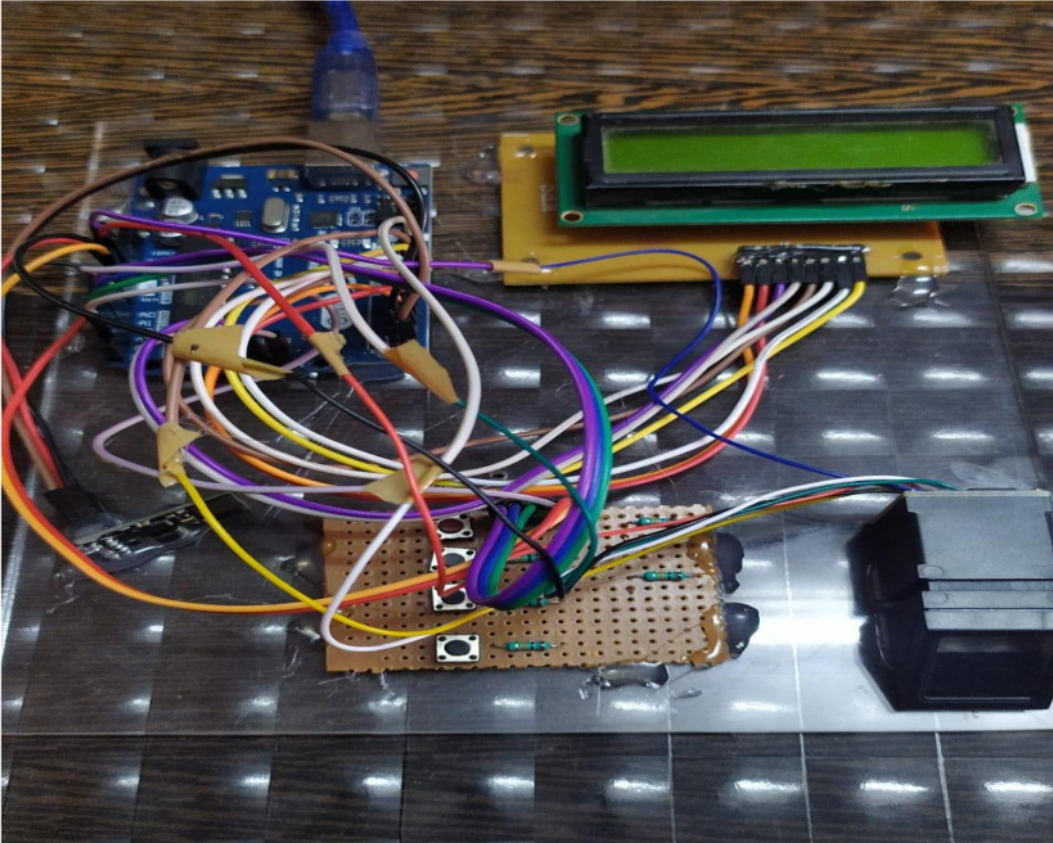


Figure 4.1: The Voting Interface Implementation

PowerUnit

This generates the power required for the devices to operate in a good working condition. It also powers some LEDs for indication purposes. It contains a 12V battery to supply power to the devices in the absence of external power.

The input to the power unit is a 220V AC which is stepped down and converted to DC. This output is used to power the screen 16 * 2 width module and the arduino uno.

LCD Screen

The LCD screen provides a means of interacting with the device. Its powered directly by a 5V power supply from the power unit.

The screen 16 * 2 width is connected to the arduino uno via an HDMI cable for receiving video streams from the arduino uno for display and a USB cable for transmitting input received from user touch to the arduino uno. The controller directly communicates with the arduino operating system running on the arduino uno enabling input to the screen sensor to be interpreted properly.

Control Unit

The control unit is the heart of the system. It is a arduino uno software. The operating system provides the resources necessary to generate a graphical user interface for the application. It also provides low level libraries to enable easy integration with other peripheral (hardware) devices.

It communicates with the card reader, the fingerprint sensor and the screen 16 * 2 width via its USB ports which serves as a source of power to some of the peripherals like the fingerprint and the card reader.

The voting application or software written in java and python, runs on this operating system and communicates with the peripheral devices by using the low level libraries provided by the operation system.

Table 4.1: Unit test for Control Unit

Test	Steps	Expected Result	Test Result
Arduino uno power	Plug the arduino uno power cord to a power source	The LED on the arduino should come on	The LED came on

Arduino uno OS boot	Put the hdmi cable in the arduino uno and power on the arduino uno	The LED on the arduino uno should come on	TheLED came on
Start Application	Attempt to run the vote application	The application should run without errors	The application ran without errors

FingerprintScanner

This is the second means by which the system authenticates a voter. It exposes four pins of which two (the RX and TX) are for serial TTL communication while the other two provides the power supply. The fingerprint sensor is connected to the arduino uno USB port through a TTL-USB converter which also provides enough voltage (5V) to power it. The fingerprint sensor is controlled by a python program which provides a wrapper for the low level libraries that communicates with it. The codes used for this communication is found in the appendixC.

Table 4.2: Unit test for the Fingerprint Scanner

Test	Steps	Expected Result	Test Result
Correct connection	Connect the pins of the finger print scanner to the appropriate pins of the arduino uno	The LED fingerprint scanner should blink .	The LED of the fingerprint blinked .

4.2 System Integration and Testing

All the different units explained above where put together such that the fingerprint scanner, camera and smart cart reader writer for the registration was added to the registration platform running on a Windows system. The registration platform was also connected to the online Server.

The result website was hosted online at [E-voting Result\(https://bit.ly/32Y5z6q\)](https://bit.ly/32Y5z6q) and linked to the onlineServer.

The administrator dashboard was installed on a Windows system and linked to the online Server as well. At the voting device end, the fingerprint module is coupled to the Arduino uno, also the smart card reader and LCD screen 16 * 2 width is connected to the Arduino uno and coupled into the voting system. The battery unit is added to the voting device too and the voting software is burnt to a memory card and inserted into the Arduino uno memory card slot. The system is started up and the voting device is working.

Table 4.3: Overall System Testing

Test	Steps	Expected Result	Test Result
On/Off	Power the system on and off	On power ON, The system should correctly boot-up within 20 seconds. On power OFF, the system should shut down within 10 seconds	Expected result gotten, as system started within 15 seconds and was shut down within 7 seconds.
Register a voter	Register the finger of the voter in the arduino software.	Display Registration Successful	Registration Successful displayed
Cast vote	Place the finger on the finger print sensor, if matched the system confirms the vote with fingerprint	Screen should display "Cast your vote "	"Cast your Vote" Displayed

View election result	The result with the no. of votes for each candidate should be shown on the lcd display.	Result should show	Result is shown
----------------------	---	--------------------	-----------------



1

Figure 4.2: Results displayed on the lcd

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

The manual system of voting has failed to tackle the basic issues necessary for a trusted voting environment which has evidently driven some of its citizens to apathy.

The E-voting system was implemented to solve the proximity bottlenecks, unnecessary time delays, with very secure and accurate recording of votes. The system has been thoroughly tested in voting accuracy, ruggedness, responsiveness, battery life expectancy, and security by means of simulation and mini voting sessions to be a successful one.

It is seen that the system is fault tolerant at all end points (registration, voting platform and the server).

The voting device can last for more than 6 hours which is very sufficient for a quick system like ours.

This system will provide boundless voter participation in remote areas with very little or no cost on the voter greatly reducing apathy. Further improvements can be done on the system to increase the credibility of the votes and further reduce proximity issues.

5.2 Recommendation

The following recommendations are made for optimal performance of the system:

1. The voting device should be operated in a dry environment with a fairly stable internet connection.

The following functionalities could be added to improve on the project:

1. Internet Voting (I-voting): the use of smart phones or any internet connected device to cast votes from any location.
2. The registered cards could be integrated into other areas of citizenship authentication and identification such as drivers' license and e-governance.

5.3 Contribution to Knowledge

Many works have been done with respect to making the electoral process better by increasing voters' interest to participate in the election and based on these existing solutions, this project model introduces the concept of voting at the closest polling unit while vote is counted where it belongs.

REFERENCES

- [1] Paul David Webb, Roger Gibbins, Heinz Eulau, "Election", Encyclopaedia Britannica. [Online]. Available:<https://www.britannica.com/topic/election-political-science>. [Accessed: Aug. 05,2019].

- [2] Toba Paul Ayeni, Adebimpe Omolayo Esan, "The Impact of ICT in the Conduct of Elections in Nigeria", American Journal of Computer Science and Information Technology, February 09, 2018 . [Online]. Available:<http://www.imedpub.com/articles/the-impact-of-ict-in-the-conduct-of-elections-in-nigeria.php?aid=22211>. [Accessed: Aug. 05,2019].

- [3] ACE, E-voting, The Electoral Knowledge Network, n.d., [Online]. Available:<http://aceproject.org/ace-en/focus/e-voting/default>. [Accessed: Aug. 07,2019].

- [4] Victor Ekwealor, Inside Nigeria's first ever electronic voting exercise in Kaduna State, Techpoint Africa, May 14, 2018, [Online]. Available: <https://techpoint.africa/2018/05/14/kaduna-electronic-voting/>. [Access: Aug. 10,2019].

- [5] Seth Rosenblatt, Jason Cipriani, Two-factor authentication: What you need to know (FAQ), CNET, June 15, 2015, [Online]. Available:<https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq>. [Accessed: Aug. 10,2019].

- [6] Alexandra Petru, What is two-factor authentication (2FA)?, iPhone Backup Extractor, Oct. 08, 2017, [Online]. Available:<http://www.iphonebackupextractor.com/blog/2016/jun/3/extract-data-two-factor-authentication/>. [Accessed: Aug. 11,2019].

- [7] van Tilborg, Henk C.A.; Jajodia, Sushil, eds. (2011). *Encyclopedia of Cryptography and Security, Volume 1*. Springer Science & Business Media.p.1305.

- [8] Jason Cipriani, Seth Rosenblatt, Two-factor verification: What you need to know (FAQ), CNET, June 15, 2015, [Online]. Available:<https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq>. [Accessed: Aug. 10,2019].

- [9] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi “On the (In) Security of Mobile Two-Factor Authentication” Lecture Notes in Computer Science, pp. 365-383, Nov 2014.
- [10] Alireza Pirayesh Sabzevar, Angelos Stavrou “Universal Multi-Factor Authentication Using Graphical Passwords”, Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems. pp. 625-632, 2008.
- [11] Olufemi Sunday Adeoye “Evaluating the Performance of two-factor authentication solution in the Banking Sector” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.
- [12] Rahul Kale, Neha Gore, Kavita, Nilesh Jadhav, Swapnil Shinde “ Review Paper on Two Factor Authentication Using Mobile Phone” International Journal of Innovative research and Studies, Vol.2, Issue 5, pp. 164 - 170, May 2013.
- [13] van Tilborg, Henk C. A.; Jajodia, Sushil, eds. (2011). *Encyclopedia of Cryptography and Security, Volume 1*. Springer Science & Business Media. p. 1305.
- [14] CardLogix Corporation, Smart Card Basics, CardLogix Corporation, 2010. [Online] Available from: <http://www.smartcardbasics.com> [Accessed 1/05/19].
- [15] Tarun Agarwal, How does the Smart Card Works?, ElProCus, n.d. [Online] Available from: <https://www.elprocus.com/working-of-smart-card/> [Accessed 1/05/19].
- [16] Michael Bairanzade, Smart card integration and specifications, ASPENCORE, 2002. [Online] Available from: https://www.eetimes.com/document.asp?doc_id=1200923 [Accessed 1/05/19].
- [17] Wikipedia, Smart card, Wikipedia, Wikipedia, n.d. [Online] Available from: https://en.wikipedia.org/wiki/Smart_card [Accessed 29/04/19].
- [18] D. Maio, and D. Maltoni, “Direct gray-scale minutiae detection in fingerprints”, IEEE

Transactions Pattern Analysis and Machine Intelligence, vol. 19(1), pp. 27-40,199.

Biometric based Electronic Voting Machine using Arduino Microcontroller and Fingerprint sensor

ORIGINALITY REPORT

15%

SIMILARITY INDEX

13%

INTERNET SOURCES

0%

PUBLICATIONS

14%

STUDENT PAPERS

PRIMARY SOURCES

1

www.archive.org

Internet Source

7%

2

archive.org

Internet Source

3%

3

Submitted to Moneague College

Student Paper

1%

4

Submitted to Melbourne Institute of Business and Technology

Student Paper

1%

5

www.ihirelogistics.com

Internet Source

1%

6

Submitted to Midlands State University

Student Paper

<1%

7

www.railwayscreditunion.com.au

Internet Source

<1%

8

Submitted to Far Eastern University

Student Paper

<1%

9	Submitted to The University of the West of Scotland Student Paper	<1 %
10	www.yonghao328.com Internet Source	<1 %
11	Submitted to Kwame Nkrumah University of Science and Technology Student Paper	<1 %
12	Submitted to nsbm Student Paper	<1 %
13	Submitted to Postgraduate Schools - Limkokwing University of Creative Technology Student Paper	<1 %

Exclude quotes On
Exclude bibliography On

Exclude matches < 5 words