

بسم الله الرحمن الرحيم



## **Palestine Polytechnic University**

College of Information Technology and Computer Engineering

Computer System Engineering Department

# **Hybrid Voting System**

### **Team Members**

Omar Herbawi

Mohammad Husini

### **Supervisor**

Dr. Radwan Tahboub

2023

# Table of Contents

<b>Chapter 1: Introduction</b>	<b>6</b>
<b>1.1 Overview</b>	<b>6</b>
1.1.1 Paper ballot voting	6
1.1.2 Electronic voting	8
1.1.3 Online voting	10
1.1.4 Hybrid voting	11
<b>1.2 Motivation and importance</b>	<b>11</b>
<b>1.3 Problem analysis</b>	<b>11</b>
<b>1.4 Problem definition</b>	<b>11</b>
<b>1.5 Requirements</b>	<b>12</b>
1.5.1 Project Requirements	12
1.5.2 Security Requirements	12
<b>1.6 System Description</b>	<b>12</b>
1.7 Project Schedule (Gantt Chart)	14
<b>Chapter 2: Background</b>	<b>15</b>
<b>2.1 Overview</b>	<b>15</b>
<b>2.2 Theoretical Background</b>	<b>15</b>
<b>2.3 Literature Review</b>	<b>18</b>
<b>2.4 Summary</b>	<b>19</b>
<b>Chapter 3: System Design</b>	<b>21</b>
<b>3.1 Overview</b>	<b>21</b>
<b>3.2 Design Options and Specifications</b>	<b>21</b>
3.2.1 System options	21
3.2.2 Hardware Components	25
3.2.3 Software Components	26
<b>3.3 Design Options</b>	<b>27</b>
3.3.1 Hardware Components	27
3.3.2 Software Components	33
<b>3.4 Conceptual system description</b>	<b>34</b>
<b>3.5 Diagrams</b>	<b>36</b>
3.6 Schematic diagram	37
3.7 Summary	37
<b>Chapter 4: Implementation and Testing</b>	<b>38</b>
4.1 Overview	38
4.2 Implementation Description	38
4.2.1 Hardware Implementation Tools	38
4.2.2 Software Implementation Tools	38
4.2.3 Communication	39
4.2.4 Hardware Implementation	39

4.2.5 Software Implementation	40
4.3 Challenges	41
4.3.1 Software challenges	41
4.3.2 Hardware challenges	42
4.4 Testing	43
4.4.1 Hardware testing	43
4.4.2 Software testing	45
4.5 Validation Results	48
4.5.1 Hardware and Software Testing	48
<b>Chapter 5: Conclusion and Future Work</b>	<b>49</b>
5.1 Conclusion	49
5.2 Future work	49

## List of Tables

<b>Table 1.1 Project Gantt Chart</b>	<b>14</b>
<b>Table 3.1 Microcontroller options</b>	<b>26</b>
<b>Table 3.2 Fingerprint options</b>	<b>27</b>
<b>Table 3.3 Printer options</b>	<b>28</b>
<b>Table 3.4 Display options</b>	<b>29</b>
<b>Table 3.5 Communication Protocol options</b>	<b>30</b>
<b>Table 3.6 Status screen options</b>	<b>31</b>
<b>Table 4.1 Hardware testing</b>	<b>42</b>
<b>Table 4.2 Software testing</b>	<b>44</b>

## List of Figures

<b>Figure 1.1 Paper ballot voting steps</b>	<b>7</b>
<b>Figure 1.2 Electronic voting steps</b>	<b>9</b>
<b>Figure 1.3 Enrollment Process</b>	<b>13</b>
<b>Figure 1.4 Voting Process</b>	<b>14</b>
<b>Figure 2.1 HTTPS Protocol</b>	<b>18</b>
<b>Figure 3.1 General Block Diagram of the system</b>	<b>34</b>
<b>Figure 3.2 Sequence Diagram of the authenticating system</b>	<b>35</b>
<b>Figure 3.3 Fingerprint matching system</b>	<b>35</b>
<b>Figure 3.4 Schematic Diagram of the system</b>	<b>36</b>
<b>Figure 4.1 The project components</b>	<b>43</b>
<b>Figure 4.2 Login form</b>	<b>45</b>
<b>Figure 4.3 Election creating form</b>	<b>45</b>
<b>Figure 4.4 Account settings form</b>	<b>46</b>
<b>Figure 4.5 Elections list page</b>	<b>47</b>
<b>Figure 4.6 Voting form</b>	<b>47</b>

## إهداء

إلى من نفضلها على أنفسنا، ولم لا؛ فلقد ضحت من أجلنا

ولم تدخر جهدًا في سبيل إسعادنا على الدوام

(أمي الحبيبة).

نسير في دروب الحياة، ويبقى من يُسيطر على أذهاننا في كل مسلك يسلكه

صاحب الوجه الطيب، والأفعال الحسنة.

فلم يبخل علينا طيلة حياته

(والدي العزيز).

كما وأقدم شكري وتقديري إلى الدكاترة الأفاضل وأخص بذكر مشرف مشروع التخرج

(الدكتور رضوان طهبوب)

إلى أصدقائنا، وجميع من وقفوا بجوارنا وساعدونا بكل ما يملكون، وفي أصعدة كثيرة

نقدّم لكم هذا البحث، وأتمنى أن يحوز على رضاكم

## **Abstract**

Our main goal was to restore public trust in the election process by building a Hybrid Voting System that adeptly merges the security of paper ballot voting with the convenience of online voting. Traditional election methods have often grappled with security issues, hacks, and leaks in the past, which had weakened people's trust in these systems. To address these issues, we implemented a secure, user-friendly interface that utilizes encryption and hash functions to secure votes, along with policies and procedures to safeguard users' data. A unique feature of the system is the integration of Internet of Things (IoT) devices to ensure real-time tracking of the voting process. The system supports voting through mobile, desktop, and physical stations, increasing accessibility for all voters. Our Hybrid Voting System was put through rigorous testing and validation, showing substantial improvements in voting integrity, security, and user experience. The successful implementation of our solution was validated by significant reductions in security risks, making the process easier and more trustworthy for both users and organizers. The results indicate a marked increase in public trust, reaffirming the effectiveness of our Hybrid Voting System in enhancing the reliability of the election process.

# Chapter 1: Introduction

## 1.1 Overview

The main problem of elections is to gain people's trust and be secure enough. Historically, great efforts have been made to ensure fair and accurate elections. Well, several methods have been used to ensure this, one of them is paper ballot voting. It has been used for a long time, but times are changing. We live in the internet age, so many new ways have been made to make the whole operation easier and safer, and we're trying to improve this more.

### 1.1.1 Paper ballot voting

Paper ballot voting is the traditional and most famous form of voting. The voter should exist physically in the polling station, and it's the one currently used by governments due to its advantages [\[1\]](#).

#### What are the steps for paper ballot voting? [\[2\]](#)

1. Individuals must register for voting before they can be assigned to a voting room.
2. The voter must go to the assigned room by the election's organizers.
3. **Election officers**, who are generally volunteers, should have their temperature and alcohol checked before entering the voting center to ensure they are at full mental capacity.
4. Visit the Voter Assistance Desk (VAD) to secure your precinct and order number, and the assigned room or group.
5. The voter should introduce themselves by stating their name to the election officers and showing their personal ID. Their data should be entered by the election officers into the system, so that they won't be able to vote again in any other voting room.
6. Get the verified ballot and marking pen. Go to a private room and fill out the form by shading in the desired place under each name.
7. The voter should put the ballot paper into the transparent ballot box.

Figure 1.1 shows an illustration of these steps:

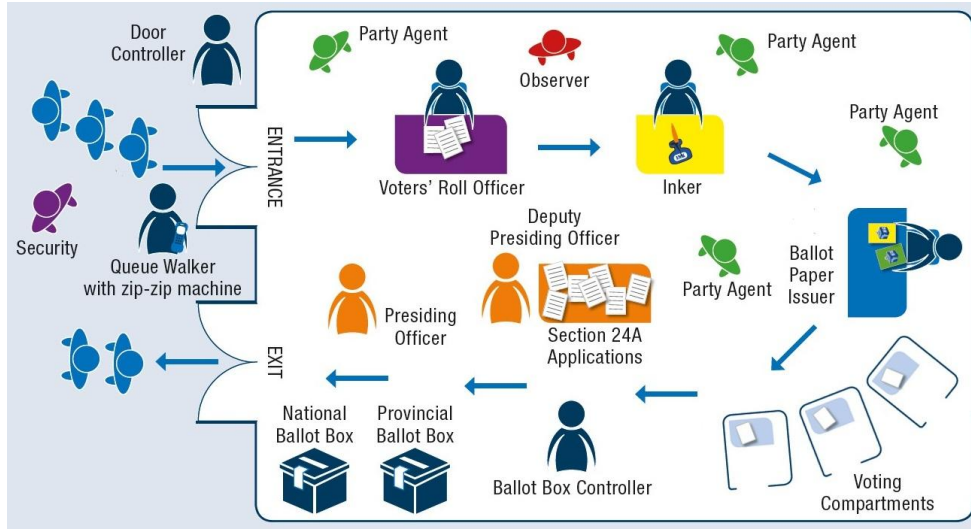


Fig. 1.1. Paper ballot voting steps

## What are the advantages and disadvantages of paper ballot voting? [\[3\]](#)

### Advantages:

- The fact that the voter exists physically in the polling station, and will put their ballot in the box with their own hand, makes this method the most trusted one
- It does not cost a lot to be implemented, which is a great advantage if we consider that the government is typically responsible for organizing elections
- It's very secure and hard to hack into.

### Disadvantages:

- Since it doesn't allow the voter to vote from the comfort of their own home. This means that if the voter is sick or cannot go to the polling station for any other reason, they will not be able to vote.



## 1.1.2 Electronic voting

The world is constantly developing, and with new technology comes new ways of doing things. Electronic voting is one example of this. Electronic voting is a newer method that is becoming more popular, and it is being used in some countries, such as India and Namibia. [\[4\]](#)

### What are the steps for electronic voting? [\[5\]](#)

1. Individuals must register for voting before they can be assigned to a voting room.
2. The voter must go to the assigned room by the election's organizers.
3. **Election officers**, who are generally volunteers, should have their temperature and alcohol checked before entering the voting center to ensure they are at full mental capacity.
4. Visit the Voter Assistance Desk (VAD) to secure your precinct and order number, and the assigned room or group.
5. The voter should introduce themselves by standing their name to the election officers and showing their personal ID. Their data should be entered into the system so that they won't be able to vote again in any other voting room or vote again.
6. The voter will be given a unique e-voting card, which is taken from a pre-printed set of e-voting cards, to identify voting sources and avoid repeated votes. Because they're pre-printed, it's impossible to identify you from any of the e-voting cards, but they do their job recording your polling station and a digital signature to prevent forgery.
7. The voter then moves to the voting booth, which contains a touchscreen computer that cannot be seen from outside the room, as well as a bar-code scanner.
8. The screen contains the candidates' names, the voter has to choose the one they want to vote for, then they will be asked to confirm the vote before officially casting it.
9. The system should count their vote, and at the end, all votes should be counted immediately.

Figure 1.2 shows an illustration of these steps:

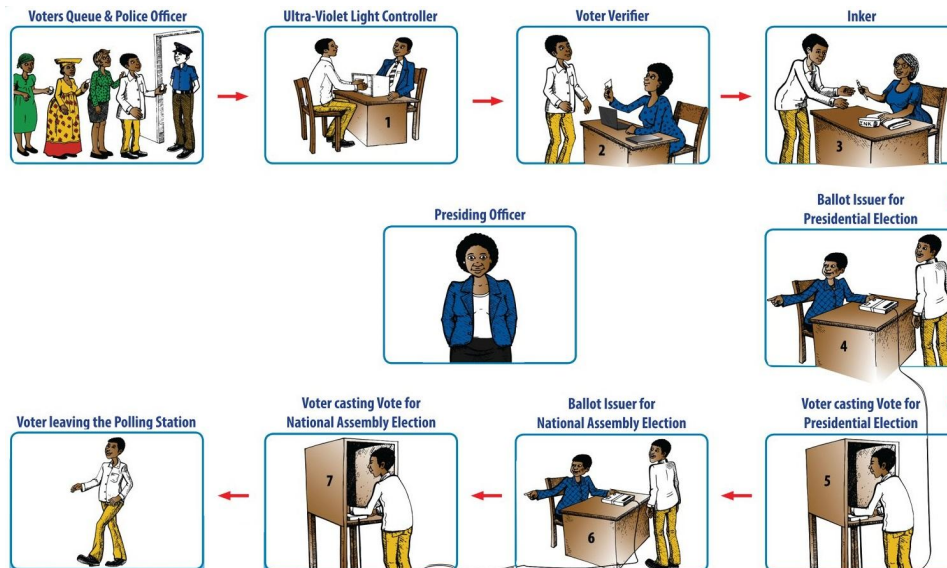


Fig. 1.2. Electronic voting steps

## What are the advantages and disadvantages of electronic voting? [6]

A great effort has been made to make the voting process easier with this method, but it has its advantages and disadvantages.

### Advantages:

- The votes are counted in no time! There's no counting by hand, so no cost is wasted on people counting votes by hand, so it saves a lot of time.
- Higher accuracy, Counting by hand is easy to manipulate and is not always accurate.

### Disadvantages:

- Nothing is 100% "unhackable" and it is not difficult to hack into a computer and change the vote
- People won't trust what they don't know. Unlike paper ballot voting, where the voter puts in a ballot by their hand in the box, in electronic voting the vote is recorded digitally.

### 1.1.3 Online voting

Some people might ask why elections aren't held online? "I can shop online. Why can't I vote online?", "Why isn't there an app that allows me to vote in my local congressional elections or even vote for president?"

#### What are the steps for online voting? [\[7\]](#)

1. User registration for the vote, by adding some personal information (such as Personal ID)
2. If the voter's fingerprint is available in the database, they will be asked to enter their fingerprint to compare them.
3. After user verification, they will have access to vote, and they can choose a candidate.
4. After they cast their vote, that vote will be anonymously counted. Their information will be encrypted and stored, so they won't be able to vote later with the same information.

#### What are the advantages and disadvantages of online voting? [\[8\]](#)

##### Advantages:

- Increasing voter participation. Since the voter can literally vote from home!
- The whole process takes no more than a minute, and it is accurate

However, the risks still far outweigh the benefits.

##### Disadvantages:

- People still don't trust what they don't know.
- Election security cannot be guaranteed because there would be too many vulnerable points in the voting system. The operating system on the voter's phone, and the servers the voter's data are stored on, even the program itself can be vulnerable.

### **1.1.4 Hybrid voting**

Well, all previous voting methods have their benefits, but in most of them, cybersecurity risks still far outweigh those benefits. This voting method combines all previous voting forms, so it's taking slices of each one (taking the important hardware and software parts) while minimizing the cybersecurity risks as possible, and getting the preliminary results of the election, and we're using a crypto processor to do all the security related algorithms (such as Homomorphic encryption, SHA-256).

The main idea of this is to have an electronic voting machine beside the paper ballot voting, so we're using electronic voting to make things easier while keeping the traditional voting methods to get people's trust.

## **1.2 Motivation and importance**

Our main motivation is to increase the trust of people and ensure that every vote is stored anonymously, so the whole voting process is as secure as possible. That the candidate who should win the election based on the votes they receive actually does, so this system improves the democratic process.

## **1.3 Problem analysis**

The need for this system comes due to the many problems in the previous voting systems, and the lack of people's trust in most of them. Mostly because of security issues, some hacks have happened in the past, which weakened people's trust in other systems. For example, in paper ballot voting, a voting fraud could happen, it's not impossible that boxes can be changed by another box full of votes of a candidate. Also, in electronic and online voting, you're not 100% sure your identity is hidden from others, that's what we're trying to solve here.

## **1.4 Problem definition**

The main problem is to make a system that is secure enough to handle the whole election process with the minimum security risk, while gaining the public's trust by still using papers.

## 1.5 Requirements

### 1.5.1 Project Requirements

Expect to build a system with the following specifications:

- The voting system must verify a voter's identity before allowing them to vote.
- The system must be able to monitor the election process and results.
- The system must be designed to accomplish the election process as smoothly as possible.

### 1.5.2 Security Requirements

Expect to build a system with the following security specifications:

- The system must send the vote's information to the database anonymously using the cryptoprocessor.
- The voting data should be sent to the crypto processor, and then the crypto processor should encrypt the data using the homomorphic encryption algorithm. This operation should be faster than the normal encryption process.
- Hashing will be used to save user-sensitive data (such as passwords), and then match them when needed.
- Homomorphic encryption will prevent anyone from seeing user-sensitive data, so the election's result will be held anonymously in the database until the election ends.
- A QR code will be used to validate the printed papers' eligibility without it being connected to the voter himself.

## 1.6 System Description

The system requirements and steps can be summarized as:

1. User registration for a vote is done through a web application. They will be asked for some information (such as their personal ID and password), and their respective fingerprint data (if available) will be fetched from the Supreme Election Commission. This information will be used to validate them, prevent identity theft, and prevent the same person from voting again, Check Figure 1.3.
2. The voter should go to the election room. The election officers will allow them to enter a private room where they will vote through a touch screen.
3. To identify the person casting the vote in the voting room, the voter must enter their registration credentials, and the system will compare them with the stored data to verify their identity.

4. Now with their identity verified, they can choose which candidate to vote for through the touch screen.
5. After confirming the vote, the system will anonymously send the vote's data (vote ID, candidate ID) to the database after encrypting it using the crypto processor with a homomorphic encryption algorithm, so the confidentiality of the vote is kept. No one will be able to see who votes to whom, and their vote will be counted correctly at the end of the election.
6. At the end of all this, the printer should print a paper with the candidate's name and QR Code to prevent box fraud, so any additional papers will be immediately detected. The voter should put this paper in the box on their way out.
7. At the end of the election, the final result of the election will be sent to the election supreme election commission, and they will be able to decrypt the final result of the election using their key to the election.

These steps are shown in Figure 1.4

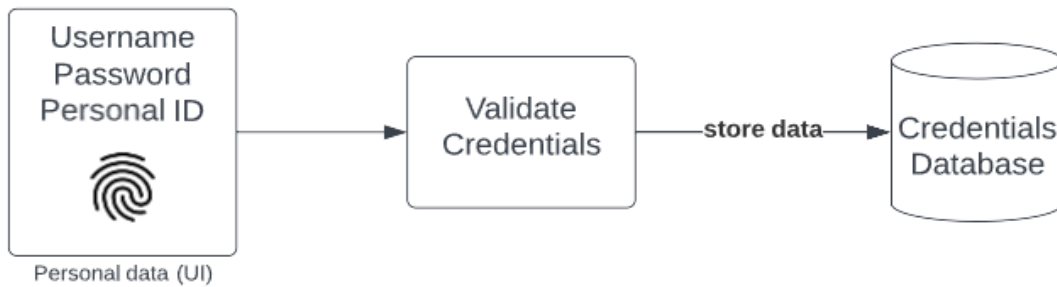


Fig. 1.3. Enrollment Process

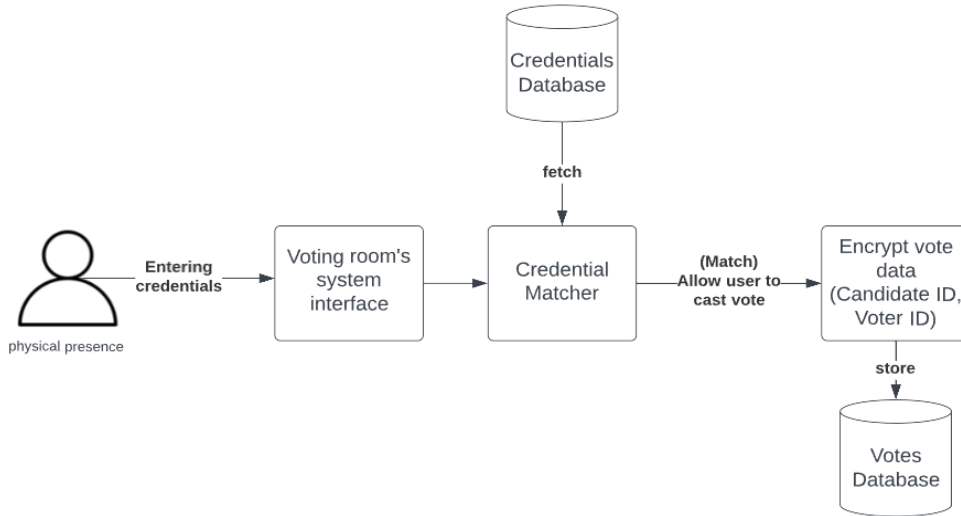


Fig. 1.4. Voting Process

## 1.7 Project Schedule (Gantt Chart)

Table. 1.1. Project Gantt Chart

Task	Duration (weeks)													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
<b>First Semester</b>														
Planning														
Research and investigation														
Requirements gathering														
System Design														
Software implementation														
Software Testing														
<b>Second Semester</b>														
Hardware implementation														
Link Hardware with software														
Testing and maintenance														

# Chapter 2: Background

## 2.1 Overview

This chapter briefly describes the theoretical background and shows the previous works about this concept and its relative projects. In the next sections, the system hardware and software components, options will be discussed.

## 2.2 Theoretical Background

Due to the vulnerabilities of today's computers and networks, the majority of governments choose not to integrate electronic tools into the operation of their democracy. Their objection stands out if the technology involves elements they have no control over. Therefore, there are still just a few nations testing voting through the Internet. Two of the few nations that have pioneered online voting and referendums are Switzerland and Estonia.

A democracy's ability to operate elections with the confidence of its voters. This is true for both traditional paper-based voting systems and hybrid voting systems, our aim is to enable voters to cast their ballots on-site too while keeping the system as strong and safe as possible.

Technologies and techniques to be used in the project would be as follows:

### 1. Security:

- **Encryption:** Data can be scrambled using encryption so that only authorized parties can decipher it. Technically speaking, it is the process of changing plaintext that can be read by humans into ciphertext, which is unreadable text. In plainer terms, encryption changes readable data to make it seem random. A cryptographic key, or collection of numbers that the sender and the recipient both have or both agreed on, can encrypt or decrypt any message [\[9\]](#). We will use it in our project to make sure the whole operation is as secure and trusted as possible, and every voter's identity is hidden from others.



- **Hash:** A hash is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length. Thus regardless of the original amount of data or file size involved, its unique hash will always be the same size. We're using the hash in our project for authentication, the username and the password should be hashed [\[10\]](#).
- **Policy:** A security policy is a document that states in writing how a company plans to protect its physical and information technology (IT) assets. Security policies are living documents that are continuously updated and changing as technologies, vulnerabilities, and security requirements change [\[11\]](#).
- **Homomorphic Encryption:** Homomorphic Encryption (HE) is distinguished by its ability to allow computations on encrypted data without needing to decrypt it first. This is invaluable in maintaining data privacy during operations. The HE schemes can be broadly classified into:
  - **Fully Homomorphic Encryption (FHE):** Supports both addition and multiplication on encrypted data.
  - **Partially Homomorphic Encryption (PHE):** Supports either addition or multiplication, but not both.

The generic form can be represented mathematically as follows:

$$E(m1) \oplus E(m2) = E(m1 + m2)$$

$$E(m1) \oplus E(m2) = E(m1 \times m2)$$

This allows for secure data manipulation without exposing the raw data.

### Paillier Homomorphic Encryption:

Paillier encryption is a type of Public Key Cryptography (PKC) and falls under the category of Partially Homomorphic Encryption (PHE) with additive properties. It's often preferred for its efficiency in additive computations.

Mathematically, given two encrypted messages C1 and C2:

$$C1 = g^{m1} r_1^n \text{ mod } n^2$$

$$C2 = g^{m2} r_2^n \text{ mod } n^2$$

The additive homomorphic property allows:

$$C1 \times C2 \text{ mod } n^2 = g^{m1+m2} (r_1 \times r_2)^n \text{ mod } n^2.$$

This property lets you perform additions on the ciphertexts  $C_1$  and  $C_2$  and get a result equivalent to  $m_1 + m_2$  when decrypted.

## 2. Software Applications:

- **Mobile Application:** A mobile application, is a kind of application software created specifically to operate on mobile devices like smartphones and tablets. Apps are often tiny, discrete software modules with constrained functionality. Thousands of apps for the iPhone, iPad, and iPod Touch are available in the App Store, which is where this usage of app software first gained popularity [\[12\]](#). In our project, the mobile application will be used to validate the QR Codes that are printed on each paper ballot.
- **Desktop Application:** A desktop application is a software program that can be run on a standalone computer to perform a specific task by an end-user [\[13\]](#). In our project, every polling room should have a standalone PC with our desktop application installed on it, which will be used to choose candidates and then cast a vote.

## 3. IOT:

The network of physical things that are implanted with sensors, software, and other technologies for the purpose of communicating and exchanging data with other devices and systems through the Internet is referred to as the Internet of Things (IoT). These gadgets include anything from common domestic items to high-tech industrial gear [\[14\]](#). In our project, every polling room must have a fingerprint sensor, The voter will be asked to scan their fingerprint, and their fingerprint should be sent to the cryptoprocessor which has internet accessibility and can match it to the one we have in the database in order to authenticate them to vote in the election.

## 4. HTTPS:

Hypertext transfer protocol secure (HTTPS) is the secure version of [HTTP](#), which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase the security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider.[\[15\]](#). Since the cryptoprocessor is connected to the internet, we're using HTTPS in our project in order to send the data securely to the server through the internet, it's

explained in Fig 2.1.

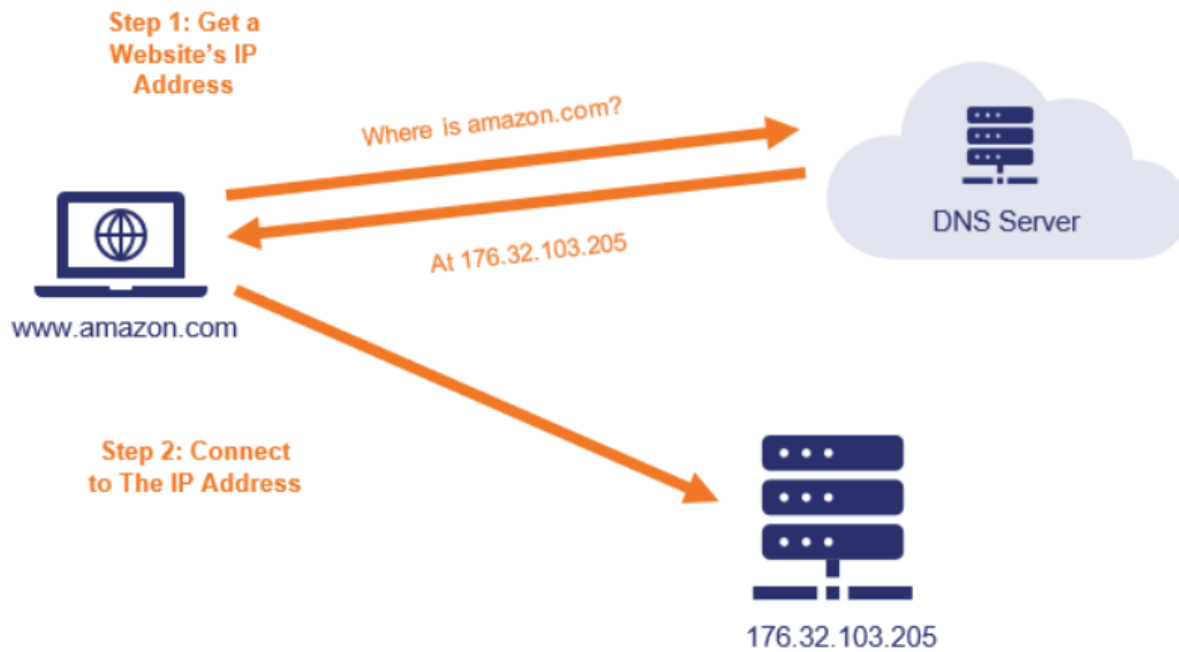


Fig. 2.1. HTTPS Protocol

## 2.3 Literature Review

This section deals with the review of past works on Hybrid Voting systems and their prediction performances.

Reference [16] proposed a voting method secured from fraudulent activity, such as falsification of results, by using Aadhaar cards (ID cards) and fingerprints. The researchers were motivated by the problem of manual checking of voter's ID card, which often led to illegal voting by false voters and multiple votes by the same voter. The objectives of the research were to design, develop, and test a fingerprint and RFID-based electronic voting system. The AT89S52 microcontroller was used and it linked with RFID tags for authentication and voting. The algorithm that integrated RFID of Aadhaar and fingerprint to achieve the authentication e-voting requirement was presented. The challenges of confidentiality, integrity, secrecy, transparency, convenience, and adaptability of e-voting functional and security requirements were not tackled.

Reference [17] The voting system used wireless technology and was based on an embedded device. The issues with rigging that result in the results being announced against the legitimate choice made by the voters and the delay in results compilation. Designing and creating a wireless system that uses fingerprint biometrics were the study's goals. To record and process ridges for authentication, a microcontroller, fingerprint scanner, and ZigBee wireless technology were incorporated. ZigBee wireless technology improved the communication of the election results, and the research led to authentication. The issues with the functional and security requirements for electronic voting, such as confidentiality, integrity, secrecy, transparency, convenience, and auditability, were not addressed. Additionally, ZigBee is an open wireless network.

Reference [18] created an online voting platform that enabled people to cast ballots via mobile applications. Issues with voters casting multiple ballots and irregularities including results at the polls being changed. Designing, putting into practice, and testing an electronic voting system that makes use of Aadhaar cards was the goal of the study. Mobile phones and Aadhaar cards were used in the methodology. Techniques for authenticating voters and confirming their votes (verifiability) by comparing their fingerprints to their Aadhaar ID were presented. The issues of privacy, secrecy, honesty, accessibility, and audibility were not resolved. Additionally, voter confirmation of ballots could encourage vote buying and selling, which would have a negative impact on the results of the election.

A lot of researchers have been trying to improve electronic voting and online voting for a very long time, but still, many problems remain unsolved, as discussed in Chapter 1. Just a few of them did research on a hybrid voting scheme, so we're fixing some of the problems that the electronic voting and online voting faced, and combining them together to make a reliable hybrid voting scheme.

## **2.4 Summary**

In this chapter, we mentioned the concepts and theoretical background of our hybrid voting scheme, and some past works on similar projects.

# Chapter 3: System Design

## 3.1 Overview

In this chapter, we will discuss the overall design of the system and the way its components are integrated together, showing the detailed conceptual description of the system and the detailed design for each component including its schematic diagram.

## 3.2 Design Options and Specifications

### 3.2.1 System options

#### 3.2.1.1 Blockchain-based system

This Hybrid Blockchain-based Voting System is designed to offer both the security of blockchain technology and the public's trust in traditional paper ballots. The voting process begins with the enrollment of voters, who are required to verify their identity and eligibility to vote.

On election day, the voter must come to the polling station to cast their vote electronically, so since their vote is saved on the blockchain, the system should use a unique digital identity for each voter that ensures that the voter can vote only once and that their vote is counted accurately. In addition, their vote is printed on a paper ballot that they can place in the polling box for backup and verification purposes.

The blockchain technology used in this system ensures the security and integrity of each vote. Each vote is recorded and stored on the blockchain, making it virtually impossible for anyone to tamper with the results. The transparency of the blockchain ensures that every vote cast is visible to anyone with access to the blockchain, making the voting process fair and democratic. The system also eliminates the need for manual vote counting and paper ballots, which saves time and money and speeds up the voting process.

The hybrid design of this system provides voters with the flexibility to register online and vote in person. This feature also ensures that voters who are not comfortable with the technology can still participate in the voting process. The use of a digital identity for each voter also prevents any attempts at voter fraud or double voting. However, the use

of blockchain technology in the system may require additional resources and training to implement and maintain. Some voters may also face technical difficulties or may not have access to the necessary technology, which could prevent them from participating in the voting process. Furthermore, there is always a risk of security breaches or hacking, which could compromise the integrity of the voting process and the security of voters' personal information.

### **Advantages:**

- **Security:** The use of blockchain technology ensures the security and integrity of each vote. Each vote is recorded and stored on the blockchain, making it virtually impossible for anyone to tamper with the results.
- **Transparency:** The transparency of the blockchain ensures that every vote cast is visible to anyone with access to the blockchain. This makes the voting process fair and democratic, as everyone can see that every vote is counted correctly.
- **Efficiency:** The use of blockchain technology eliminates the need for manual vote counting and paper ballots. This can save time and money and can help speed up the voting process.
- **Flexibility:** The hybrid design of our system allows voters to register online and vote in person, giving them the best of both worlds.

### **Disadvantages:**

- **Technical Complexity:** The blockchain technology used in our system can be complex, and it may require additional resources and training to implement and maintain the system.
- **Access to Technology:** Some voters may not have access to the necessary technology or may not be familiar with using it. This could prevent them from being able to participate in the voting process.
- **The need for miners:** Another disadvantage of establishing this system is that we will need miners who are responsible for verifying the transactions on the blockchain. These miners are required to invest computational power and resources to ensure that the votes are recorded accurately and securely. The process of mining can be time-consuming and resource-intensive, and it may require significant investment to set up the infrastructure. This could be a barrier

to the adoption of the system, particularly for smaller organizations or jurisdictions with limited resources. Additionally, the availability and reliability of miners can also impact the efficiency and effectiveness of the voting process.

### **Conclusion:**

Blockchain-based online voting systems can offer several advantages, including security, transparency, reliability, and cost-effectiveness. However, there are also several disadvantages, such as the complexity of the technology, lack of standards, and concerns about voter anonymity. Therefore, any implementation of a blockchain-based online voting system should be carefully designed and tested to ensure that it meets the highest standards of security, transparency, and reliability.

### **3.2.1.2 Zero knowledge proof-based system**

Our anonymous voting system ensures the confidentiality of voters' political preferences while providing a secure and accessible voting experience. The voter registration process happens in the polling station where the voter presents their ID to the election official. The official checks that the ID has not been used to vote before. Once registered, the voter can cast their vote anonymously. The voter data is stored and kept anonymously in the system's database. The database only records the vote itself. This information is used to calculate the final result, but there is no way to link a vote to a specific voter. This ensures that the voter's political preferences are kept confidential and protected from external scrutiny.

On the day of the election, the voter goes to the designated polling station and presents their id card to the election official. After verifying the card, the official provides the voter with a paper ballot that lists the candidates or options for the election. The voter marks their choice on the ballot and then places it in a ballot box, which acts as a backup in case of any discrepancies or challenges to the electronic data.

**Conclusion:**

Our anonymous voting system offers a simple, secure, and confidential voting experience. By checking the ID of each voter, we ensure that no voter can cast more than one vote. The use of paper ballots provides a physical record of the vote that can be audited and verified in case of any disputes or challenges to the electronic data. The anonymity of the system ensures that voters can express their political preferences without fear of retribution or discrimination. The voter registration process and physical polling stations make our system accessible to all eligible voters, while ensuring the integrity and security of the voting process.

**Advantages:**

- **Confidentiality:** The anonymity of our system ensures that voters can express their political preferences without fear of retribution or discrimination.
- **Accessibility:** The online registration process and physical polling stations make our system accessible to all eligible voters, including those who may not have access to technology or the Internet.
- **Simplicity:** The system is easy to use, and the electronic and paper voting options provide flexibility for voters who may prefer one method over the other.
- **Security:** The use of paper ballots ensures that there is a physical record of the vote that can be audited and verified in case of any disputes or challenges to the electronic data.

**Disadvantages:**

- **Vote Manipulation:** The system is susceptible to voter fraud and manipulation, as there is no way to verify the identity of the voter or prevent them from voting multiple times. This risk can be mitigated by implementing rigorous security protocols, such as regular audits and the use of physical ballot boxes.
- **Counting Accuracy:** The use of a database to record the votes can be susceptible to errors or technical glitches, which can affect the accuracy of the final result. This risk can be minimized by implementing redundancy and backup systems, as well as thorough testing and quality assurance processes.



- **Cost:** The system requires significant investment in technology, infrastructure, and personnel to maintain and operate. This cost may be a barrier to adoption, particularly for smaller organizations or jurisdictions with limited resources.

### 3.2.1.3 Our choice

We've clearly chosen our system over those two, because of the advantages and the disadvantages of the two described above, and their over-complexity of them.

## 3.2.2 Hardware Components

- **Microcontroller:**

We need two microcontrollers to deal with the data received from the connected sensors, for example one should be able to receive data from the fingerprint sensor then hash the data and pass it to the central microcontroller (crypto processor) that is able to deal with the data and do the necessary security algorithms on them, then send them database if needed.

We chose the **ESP32** as the microcontroller that should read data from sensors (such as the fingerprint sensor) since it's the one that fulfills our requirements for that job, due to its cost and capability of reading the fingerprint, which makes data transition much easier, also it's so easy to manage input/output signals and to connect the sensor.

We've chosen the FPGA as a cryptoprocessor due to its speed and capability of doing crypto algorithms faster than the normal device would do.

- **Fingerprint scanner:**

To prevent impersonation (A voter claims to be another one), we're using a fingerprint scanner to compare a voter's fingerprint in the voting room with our stored one. The microcontroller will be used to hash the fingerprint before comparing it.

The **flashtree FPM12 optical fingerprint scanner** is the most common one and it fulfills our mentioned requirements and has good accuracy.

- **Printer:**

To prevent voting fraud (false votes), the printer should print a ballot paper that contains the candidate's name and a unique QR Code that could be scanned later to make sure the vote is cast correctly. The need for fast printing and since the data to be printed are just some lines makes the **BESTEASY Thermal Label Printer** the best choice, for its cheap price and availability.

- **Display:**

There should be a display in each voting room to show the interface that allows the user to communicate with our system in real-time.

Any display would do the job, but a touch screen would be better, we choose the most common and available one which is a normal **Tablet Monitor**.

- **Communication Protocol:**

Since we're transferring data through WiFi and the local network, a fast and secure communication protocol should be used. That's why we're using the HTTPS protocol.

- **QR Scanner:**

To prevent voting fraud, we need to make sure that every ballot paper is true and that there were no additional papers put by anyone in the ballot box. In order to do this, we need to scan every ballot paper's QR Code and make sure it's not duplicated and it's a valid one.

### 3.2.3 Software Components

- **Integrated Development Environment:**


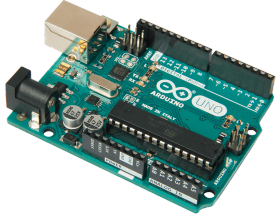

Since we're using ESP32 which supports Arduino commands, Arduino IDE would be a great choice, the main problem here is, what if we want to implement some libraries such as the **Fingerprint reader library**? Here comes what we call PlatformIO, which helps developers implement libraries much easier and faster and provides a huge collection of libraries. We're using **Visual Studio Code** since it's the only IDE that supports PlatformIO.

## 3.3 Design Options

### 3.3.1 Hardware Components

- **Microcontroller:**




Table. 3.1. Microcontroller options

Microcontroller		
Type	Image	Specifications
Raspberry PI		<ul style="list-style-type: none"><li>● High cost.</li><li>● Small size.</li><li>● Suitable to install.</li><li>● Cables needed for communication.</li><li>● More computational power than we need.</li></ul>
Arduino Uno		<ul style="list-style-type: none"><li>● Low cost.</li><li>● Small size.</li><li>● Suitable to install.</li><li>● Limited memory on board makes creating complex stuff hard.</li></ul>
ESP32		<ul style="list-style-type: none"><li>● Low cost.</li><li>● Small size.</li><li>● Built-in Wifi &amp; Bluetooth.</li><li>● Suitable for complex operations.</li><li>● Easy to set up and implement.</li></ul>

Raspberry PI is available at higher costs so it's out of the equation, Arduino Uno doesn't support PlatformIO, the only left microcontroller is ESP32.

- **Fingerprint scanner:**




Table. 3.2. Fingerprint options

Fingerprint scanner		
Type	Image	Specifications
<b>Kensington VeriMark Thermal Fingerprint Reader</b>		<ul style="list-style-type: none"> <li>● Use heat to create the image of your fingerprint.</li> <li>● A temperature difference must exist between your finger and room temperature.</li> <li>● Most accurate.</li> </ul>
<b>Invento R305 Optical Biometric Fingerprint Sensor</b>		<ul style="list-style-type: none"> <li>● Use an LED bulb to illuminate the finger, so light and dark areas are created by the ridges of your finger.</li> <li>● Stray light from another source may reduce the accuracy.</li> <li>● Most Common.</li> </ul>
<b>Fingerprint Identification Module, Capacitive Fingerprint Recognition Module</b>		<ul style="list-style-type: none"> <li>● Use capacitors and thus electrical current to form an image of the fingerprint.</li> <li>● Fast verification.</li> <li>● Allows to freely input/output fingerprint images.</li> <li>● Most stable.</li> </ul>

We need something accurate and with a suitable price and available in markets, the only one with this is the optical sensor.

● **Printer:**

Table. 3.3. Printer options

Printer		
Type	Image	Specifications
<b>BESTEASY Thermal Label Printer</b>		<ul style="list-style-type: none"> <li>● Faster printing speed.</li> <li>● Small size.</li> <li>● Prints only what is needed</li> </ul>
<b>LabelRange LP320 Label Printer</b>		<ul style="list-style-type: none"> <li>● Better color options and Higher image resolution.</li> </ul>
<b>Brother MFC-J1010DW Wireless Color Inkjet</b>		<ul style="list-style-type: none"> <li>● High cost for the printer itself and the Inject ink.</li> <li>● Has a lot of moving parts increasing the chance of breakdowns.</li> <li>● Data written on paper is risk of forgery because it uses Ink.</li> </ul>

Inkjet printers are very common and printers like these are available literally in almost every company (unlike the other ones), due to the fact that we're using it.

- **Display:**




Table. 3.4. Display options

Display		
Type	Image	Specifications
Treedix 3.5 inch TFT LCD Display		<ul style="list-style-type: none"> <li>● High cost.</li> <li>● Not very common.</li> </ul>
Longruner 7 Inch Capacitive Touch Screen TFT		<ul style="list-style-type: none"> <li>● Most expensive.</li> <li>● It is difficult to provide.</li> </ul>
Tablet Monitor		<ul style="list-style-type: none"> <li>● Manageable cost.</li> <li>● Most common and easy to provide one of those.</li> </ul>

Any monitor can be used here but Computer Monitors are the most available ones


- **Communication Protocols:**

Table. 3.5. Communication Protocol options

Communication Protocol		
Type	Image	Specifications
MQTT		<ul style="list-style-type: none"> <li>● Security isn't built-in, so comes to the end-user to set their security constraints.</li> <li>● Short specification for the developers (CONNECT, PUBLISH, ...).</li> <li>● MQTT has a very short message header and the smallest packet message size of 2 bytes.</li> </ul>
HTTPS		<ul style="list-style-type: none"> <li>● Human readability</li> <li>● provides easier debugging for developers.</li> <li>● More common</li> </ul>
LwM2M		<ul style="list-style-type: none"> <li>● UDP is used in LWM2M which does not guarantee delivery of the datagrams</li> <li>● It is designed to manage low-cost and more constrained devices.</li> </ul>

- **Status Screen**

Table. 3.1. Status screen options

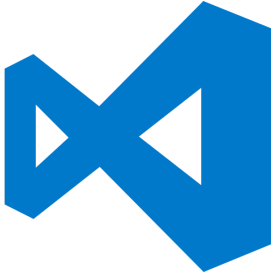

QR Scanner		
Type	Image	Specifications
2 Inch status screen		<ul style="list-style-type: none"> <li>● Low cost</li> <li>● Enough for the job</li> <li>● Will reduce wasted time spent trying to read bad QR Codes</li> <li>● Minimize the risk of fraud</li> </ul>



### 3.3.2 Software Components

- **Integrated Development Environment:**

Table. 3.6. Integrated Development Environment options

Integrated Development Environment		
Type	Image	Specifications
Visual Studio Code		<ul style="list-style-type: none"> <li>● Much easier to deal with</li> <li>● Supports a huge collection of libraries.</li> <li>● Supports PlatformIO.</li> <li>● Better overall features and performance.</li> <li>● Not easy for testing.</li> </ul>
Arduino IDE		<ul style="list-style-type: none"> <li>● Made specifically for Arduino and provides easier testing methods.</li> <li>● Doesn't support PlatformIO so there are no additional libraries.</li> </ul>

### 3.4 Conceptual system description

The system consists of a number of steps that should be followed in order to establish a fair election process, so that the one who should win is the one who actually does.

The first step is the registration process, It's the only one that can be done using the internet and without the need to be physically present in the polling station, The user will be asked for some personal information such as ID, Full Name, Fingerprint, etc .., this data will be encrypted on the client side and directly sent to the secured cloud server as shown in Fig 3.2.

After the user has registered themselves into our system, and since the system can run multiple elections at the same time, they will have to enroll themselves into one of the running elections, The user should visit one of the polling stations available in their area to cast their vote.

and here comes the next step, when the user arrives at the polling station, they will be welcomed with a screen in that polling station that is waiting for them to enter their credentials (identification and password) (password can be entered using a physical num pad connected to the ESP as shown in Fig. 3.4). After they enters them, they will be immediately hashed using SHA-256 hashing algorithm then directly sent to the secured cloud server, the cloud server will have to compare this data with the one already stored, and send a success or fail signal to the polling station as shown in Fig. 3.1, Fig 3.3.

And since everything in our system has its own public/private key (from individuals to the voting machines), all the communications will be secure between the client and the server (using HTTPS), to accomplish confidentiality for example, in case if the polling station wants to send a message to the main server, it has to encrypt the message using the public key to the server, so the only one that can actually decrypt that message is the server, that's basically the job of the HTTPS protocol, but that doesn't prevent anyone in the middle to edit that message content, to accomplish integrity too, a hash should be sent with every communication between the client and the server.

Since the system can run multiple elections at the same time, it creates a new table for every new election, for example, if someone created an election with id (#153913) a new table should be created with the name "election\_153913" and should have the following fields (voter\_token, candidate\_1, candidate\_2, candidate\_3, candidate\_n), so when the server receives the vote request from the polling station, it destructs it so that the request can fit that structure.

Then the voting step comes, When the voter is authenticated and authorized to vote, they will be able to choose their representers on the screen and then click on the voting button, after

that the polling station should generate a request that looks like this (voter\_token, candidate\_1, candidate\_2, candidate\_3, candidate\_n), for example, if the voter with the id 21245 votes for candidate 2, the request will look like this (21245, 0, 1, 0, 0), which means that when the server should count the votes of candidate\_2, it should add 1 to them and should add 0 (nothing) to the other candidates, after that the polling station sends this request to the central server.

When this request reaches the server, it destroys it to fit the structure of the election table and immediately inserts it there so that it can be counted later, after this the server sends a successful response to the polling station.

Finally, the Microcontroller will send a request to the printer printing the vote id and the validation code so it can be checked anytime later that the vote has been counted correctly.

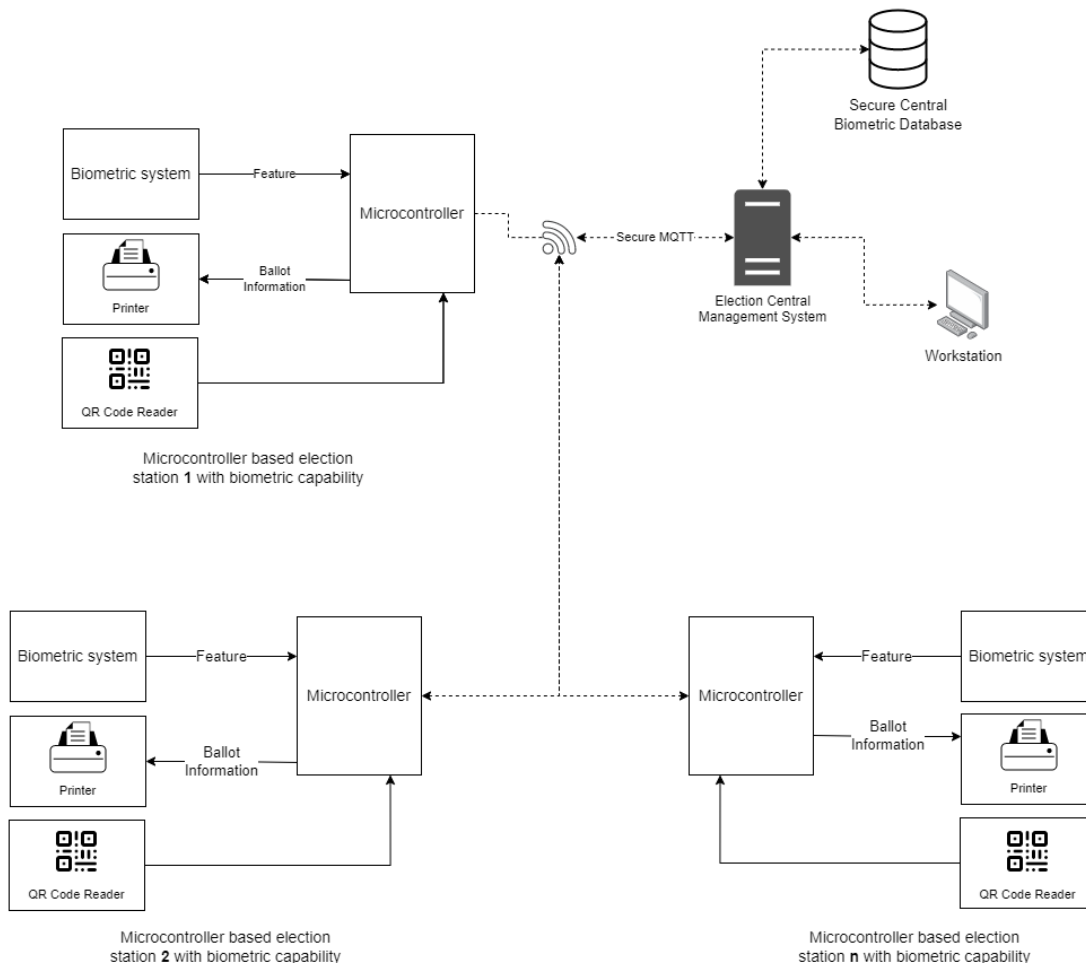


Fig. 3.1. General Block Diagram of the system

### 3.5 Diagrams

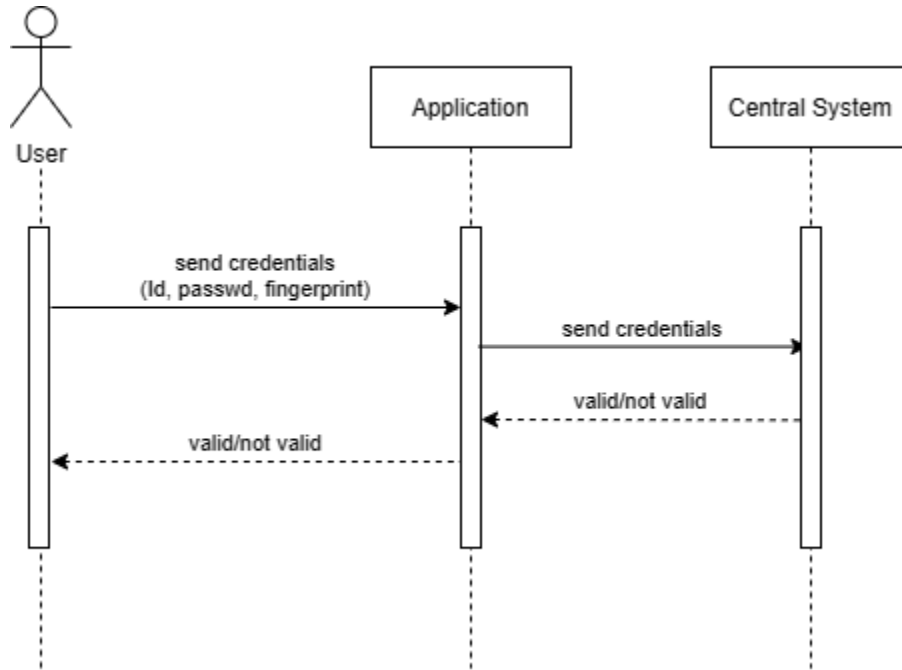


Fig. 3.2. Sequence Diagram of the authenticating system

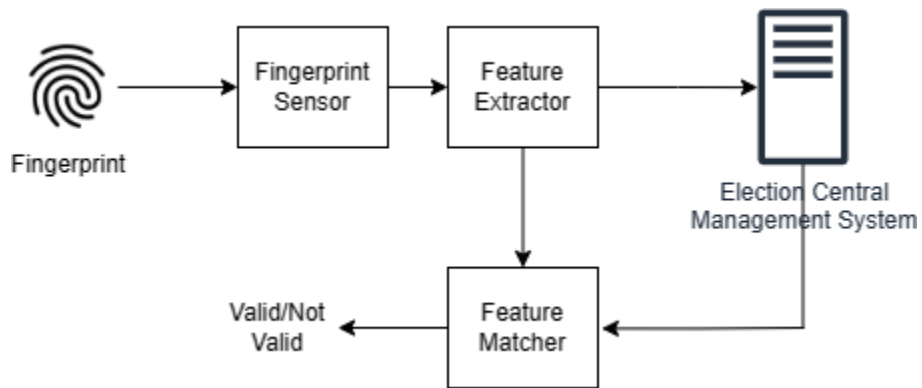


Fig. 3.3. Fingerprint matching system

### 3.6 Schematic diagram

The main components that appear in the block diagram are shown here

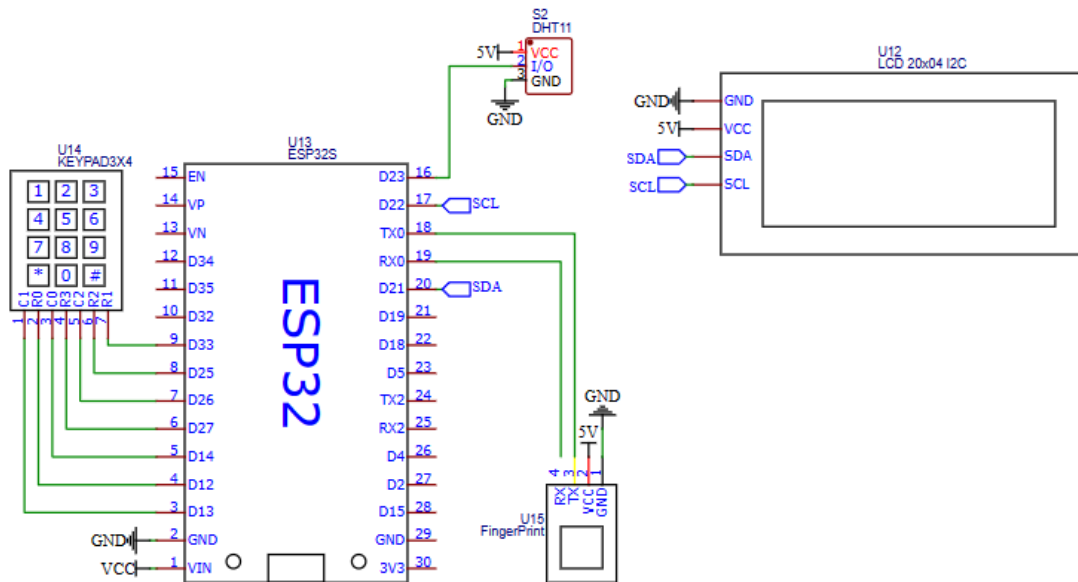


Fig. 3.4. Schematic Diagram of the system

### 3.7 Summary

A hybrid voting system combines online and paper ballot voting. It allows voters to cast their ballots either through an online platform or at a polling station. This type of system can increase accessibility and potentially reduce the risk of fraud, but it also requires secure online infrastructure and can be vulnerable to technical issues. It is important for election officials to carefully consider the risks and benefits of using a hybrid voting system and ensure the integrity of the election.

# Chapter 4: Implementation and Testing

## 4.1 Overview

In this chapter, we delve into the process of implementation, detailing the hardware and software tools used to bring our system to life. We also outline the challenges encountered during the implementation phase, both on the hardware and software fronts.

## 4.2 Implementation Description

### 4.2.1 Hardware Implementation Tools

To facilitate the hardware implementation of our system, we used various tools, some of which are mentioned below.

1. **Secure Printers:** To print paper ballots that are needed for the hybrid system. These printers should have the capability to print secure features like barcodes or QR codes.
2. **IoT Devices:** To monitor and track the process of voting in real time. IoT sensors can be employed to track the transport and handling of paper ballots.
3. **Voting Terminals:** These will serve as physical interfaces for voters to cast their votes. They need to be user-friendly and secure.

### 4.2.2 Software Implementation Tools

The implementation of the Hybrid Voting System involved the utilization of various software tools to develop the necessary components. The key software implementation tools employed in the project include:

1. **Programming Languages:** The system was developed using a combination of programming languages such as NodeJS, ReactJS, and HTML/CSS. NodeJS was primarily used for the backend server-side programming, while ReactJS and HTML/CSS were utilized for the development of the voting machine user interfaces.
2. **Integrated Development Environments (IDEs):** Different IDEs were employed to facilitate the software development process. These included only VSCode, which provided a comprehensive set of tools and features to enhance code development, debugging, and deployment.
3. **Database Management Systems:** A database management system (MySQL) was employed to store and manage the voter registration data, candidate information, and

vote records securely. Structured Query Language (SQL) was used to interact with the database and perform necessary operations such as data retrieval, insertion, and updating.

### 4.2.3 Communication

The Hybrid Voting System required seamless and secure communication between the voting machines and the central server. The following communication methods were implemented:

1. **Local Network Communication:** The voting machines and the central server were connected via a local network infrastructure. This facilitated the transmission of encrypted vote data and ensured real-time synchronization between the machines and the server, each voting room has an ESP32 in it, that is used to scan the fingerprint from the user, then send the data to the central Raspberry PI, which works as a crypto processor, that can hash and compare the scanned fingerprint.
2. **Transport Layer Security (TLS):** To enhance the security of data transmission, TLS encryption was employed. This encryption protocol ensured that the vote data exchanged between the voting machines and the central server remained confidential and protected from unauthorized access.

### 4.2.4 Hardware Implementation

Implementing the hardware involved assembling all the necessary components according to our system design. First, we tested the microcontrollers (ESP32 and Raspberry PI), the fingerprint scanner, and the printer. We then connected the display to the microcontrollers using the appropriate interface cables. Once all the components were in place, we ran a series of tests to verify that they were working as intended. These tests included checking voltage levels with a multimeter, inspecting signal integrity with an oscilloscope, and confirming that the fingerprint scanner and printer could communicate effectively with the microcontrollers.

## 4.2.5 Software Implementation

For software implementation, we are using Visual Studio Code with the PlatformIO plugin, as it is an IDE that supports a wide range of programming languages and has robust support for the ESP32 microcontroller. First, we wrote the program for the ESP32 microcontroller to interact with the fingerprint scanner, printer, and display. This included writing the firmware for the fingerprint scanner, which involved converting the scanned fingerprints into a hash code that can be compared with the stored fingerprints in the database. For the crypto processor, we implemented cryptographic algorithms using Python. These algorithms are used to encrypt and decrypt the data transmitted between the ESP32 and the central database. Next, we implemented the software for the server that runs the central database. This server software is responsible for storing and retrieving voter information, verifying the hashed fingerprints from the ESP32, and recording the votes. Finally, we tested each component of the software separately to ensure they function as expected. We also tested the whole system to ensure that all components worked together correctly.



## 4.3 Challenges

### 4.3.1 Software challenges

During the implementation of the Hybrid Voting System, several issues and challenges were encountered. These included:

1. **Data Privacy and Security:** Safeguarding voter's biometric data is crucial. The software has to be designed to protect this sensitive data both during transmission (using robust encryption techniques) and at rest in the central database.
2. **Real-Time Processing:** The system should be able to process fingerprint data, compare it with stored data, and authenticate voters in real time to avoid long queues at voting stations.
3. **Database Management:** The central database will store a vast amount of data. Efficient database management techniques should be implemented to ensure quick retrieval and update of records.
4. **Error Management and Redundancy:** Ensuring robust error management, redundancy, and fail-safe mechanisms to prevent loss of data or system failures due to unexpected issues.
5. **Software Compatibility and Integration:** Ensuring that the software components work well together and are compatible with the different hardware components can be challenging. This includes the firmware for the fingerprint scanner, the cryptographic processor, the ESP32 microcontroller, and the server software.
6. **Scalability:** The software should be scalable to handle a large number of simultaneous voters, especially during peak voting hours.
7. **User Interface Design:** Since the system would be used by voters with varying technical proficiency, ensuring the software interface is user-friendly and intuitive is a challenge.
8. **Updating and Maintenance:** Providing regular software updates for enhanced security features or to fix bugs, and ensuring these updates can be implemented seamlessly without disrupting the service.

### 4.3.2 Hardware challenges

During the implementation of the Hybrid Voting System, several issues and challenges were encountered. These included:

1. **Biometric Reader Integration:** Designing an efficient and reliable fingerprint scanner that can accurately capture and convert biometric data into a suitable format for processing can be challenging.
2. **Hardware Security:** Ensuring that the fingerprint scanner, cryptographic processor, and other hardware components are tamper-resistant and can withstand potential security threats is a significant challenge.
3. **Power Supply Management:** Ensuring reliable power supply management for field devices like fingerprint scanners, which might be used in locations where power supply is irregular.
4. **Interoperability of Devices:** The system includes a variety of devices such as the ESP32 microcontroller, a printer, and a display. Each of these devices may use different communication protocols, making their seamless integration challenging.
5. **Environment Conditions:** The durability and functionality of hardware components like fingerprint scanners in diverse environmental conditions (dusty or humid environments, varying temperatures, etc.) could pose a challenge

## 4.4 Testing

### 4.4.1 Hardware testing

During the implementation of the Hybrid Voting System, several issues and challenges were encountered. These included:

Table. 4.1. Hardware testing

<b>Case</b>	<b>Expected Output</b>	<b>Obtained Output</b>	<b>Pass/Fail</b>
Internet Connection Test	Successful connection to the internet	Connected to the internet	Pass
Database Connection Test	Successful connection to the database	Successful connection to the database	Pass
ESP32 Connection Test	ESP32 Connection Test	ESP32 Connection Test	Pass
ReactJS App to Crypto Processor Test	Successful connection to the Crypto Processor	Connected to the Crypto Processor	Pass
Biometric Data Transmission Test	Successful transmission of fingerprint data to the Crypto Processor	Fingerprint data transmitted successfully	Pass
Fingerprint Status Screen Test	Proper display of the Fingerprint current status	Status displayed correctly	Pass



Fig. 4.1. The project components

## 4.4.2 Software testing

During the implementation of the Hybrid Voting System, several issues and challenges were encountered. These included:

Table. 4.2. Software testing

<b>Case</b>	<b>Expected Output</b>	<b>Obtained Output</b>	<b>Pass/Fail</b>
Login Authentication Test	Successful login/authentication	Logged in successfully secured	Pass
Fetching Data from Database Test	Successful retrieval of data from the database	Data fetched correctly	Pass
ReactJS App to ESP32 Communication Test	Successful retrieval of data from the database	Communication established correctly	Pass
Biometric Validation Test	Successful validation of biometric data	Biometric data validated correctly	Pass
Encryption and Hashing Test	Proper encryption and hashing of sensitive data	Data encrypted and hashed correctly	Pass
Security Test	System security measures in place	System security measures effective	Pass

**Login form:** this page is used to authenticate users to the website, and giving them their respective permissions depends on their identity.

The login form is split into two vertical panels. The left panel is white and features the heading 'WELCOME' in bold black text. Below it are two input fields: 'National ID' and 'Password'. A blue 'Login' button is centered below the fields. At the bottom of the white panel is the text 'Don't have an account?'. The right panel is blue and features the heading 'SCAN QR CODE' in white text. In the center is a large QR code. Below the QR code, it says 'Use the mobile application to scan this QR Code'.

Fig. 4.2. Login form

**Election creating page:** This page is used to create elections, only authorized users by admins, should be able to create new elections or delete their existing elections.

**ACCOUNT SETTINGS**

The form is titled 'General Information' and includes a 'Save' button in the top right. Below the title is the text 'Here's the basic knowledge about your election.' The form contains several input fields: 'ELECTION NAME' and 'ELECTION TYPE' are side-by-side text boxes; 'ELECTION DESCRIPTION' is a larger text area; 'ELECTION DATE' is a date range selector with 'Start date', 'End date', and a calendar icon; 'NUMBER OF CANDIDATES' is a numeric input with minus, zero, and plus buttons. At the bottom, there is an orange warning box with an exclamation mark icon and the text 'Full this information faithfully, for fair elections.', followed by a 'Next' button.

Fig. 4.3. Election creating form

**Account settings page:** the user should be able to edit their basic account settings from this form.

The form is titled "Your Information" and includes the subtitle "Here's our basic knowledge about you." and a "Save" button in the top right corner. It contains four input fields: "FIRST NAME", "LAST NAME", "EMAIL", and "PASSWORD". Below the fields is an orange notification bar with a warning icon and the text "We will never spam your email! Whatsoever."

Fig. 4.4. Account settings form

**the Elections list page:** The user should be able to view elections from here.

The page features a heading "Just Finished" with a trophy icon and a "Sort" button. Below are three election cards, each with a calendar icon and "1d" indicating the time since the election. The first card is titled "Test Election" with candidates "123456789001 vs. 123456789002", "Winner: Not determined yet", and "2 Votes". The second card is titled "Official Election" with candidates "Ahmad vs. Mohammad vs. Ali", "Winner: Not determined yet", and "0 Votes". The third card is titled "test123" with candidates "ahmad vs. mohammad", "Winner: Not determined yet", and "0 Votes".

Fig. 4.5. Elections list page

**Voting page:** The user should be able to choose their representatives and vote from here.

**PLEASE SELECT YOUR REPRESENTERS**  
**YOU HAVE 1 MORE VOTES**

The image displays a voting interface. At the top, the text reads "PLEASE SELECT YOUR REPRESENTERS" and "YOU HAVE 1 MORE VOTES". Below this, there are two candidate cards. Each card features a circular profile icon with a person silhouette, a unique ID number (123456789001 and 123456789002), the text "Candidate Description", and a blue "SELECT" button. At the bottom center of the interface is a blue "Proceed" button with an upward-pointing arrow.

Fig. 4.6. Voting form

## 4.5 Validation Results

### 4.5.1 Hardware and Software Testing

To validate the functionality and performance of the hardware and software components used in the system, comprehensive hardware testing was conducted successfully.



# Chapter 5: Conclusion and Future Work

## 5.1 Conclusion

We successfully designed a Hybrid Voting System aimed at merging the integrity of paper-based systems with the convenience of digital voting. Our system enhances user experience, ensures secure and anonymous voting through encryption and hashing, and supports real-time monitoring via IoT devices. Rigorous testing has validated significant improvements in security and increased public trust in the electoral process.

## 5.2 Future work

Explore scalability, investigate advanced encryption, enhance UX through machine learning, consider blockchain for decentralization, and conduct real-world pilot tests.

## References

- [1] "Ballot paper," Polyas, 2022. [Online]. Available: <https://www.polyas.com/election-glossary/ballot-paper>. [Accessed: Nov. 2022].
- [2] "Voting Process," Electoral Commission of South Africa, 2022. [Online]. Available: <https://www.elections.org.za/pw/Elections-And-Results/VotiBallot Paper explained in the Election Glossary!ng-Process>. [Accessed: Dec. 2022].
- [3] "Advantages & Disadvantages of Paper Ballot Voting," World Blaze, 2022. [Online]. Available: <https://www.worldblaze.in/advantages-disadvantages-of-paper-ballot-voting/>. [Accessed: Dec. 2022].
- [4] A. Jain and S. Trehan, "How electronic voting machines have improved India's democracy," TechTank, Brookings, 6 Dec. 2019. [Online]. Available: <https://www.brookings.edu/blog/techtank/2019/12/06/how-electronic-voting-machines-have-improved-indias-democracy/>. [Accessed: Dec. 2022].
- [5] "The electronic voting process," Elections ACT, 2022. [Online]. Available: [https://www.elections.act.gov.au/elections\\_and\\_voting/electronic\\_voting\\_and\\_counting/the\\_electronic\\_voting\\_process](https://www.elections.act.gov.au/elections_and_voting/electronic_voting_and_counting/the_electronic_voting_process). [Accessed: Jan. 2023].
- [6] D. Leclair, "How Electronic Voting Works: Pros and Cons vs. Paper Voting," MakeUseOf, 2022. [Online]. Available: <https://www.makeuseof.com/tag/how-electronic-voting-works/>. [Accessed: Jan. 2023].
- [7] "4 Easy Steps for Online Voting in Union Elections," Survey & Ballot Systems, 2022. [Online]. Available: <https://www.surveyandballotsystems.com/blog/best-practices/online-voting/4-easy-steps-for-online-voting-in-union-elections/>. [Accessed: Jan. 2023].
- [8] "The Advantages and Disadvantages of Online Voting Systems," ElectionBuddy, 20 Apr. 2022. [Online]. Available: <https://electionbuddy.com/blog/2022/04/20/the-advantages-and-disadvantages-of-online-voting-systems/>. [Accessed: Feb. 2023].
- [9] "What Is Encryption?," Cloudflare, 2022. [Online]. Available: <https://www.cloudflare.com/learning/ssl/what-is-encryption/>. [Accessed: Feb. 2023].
- [10] "Hash," Investopedia, 2022. [Online]. Available: <https://www.investopedia.com/terms/h/hash.asp>. [Accessed: Feb. 2023].
- [11] "What is security policy? - Definition," TechTarget, 2022. [Online]. Available: <https://www.techtarget.com/searchsecurity/definition/security-policy>. [Accessed: Feb. 2023].

- [12] "Mobile Application (Mobile App) Definition," Techopedia, 2022. [Online]. Available: <https://www.techopedia.com/definition/2953/mobile-application-mobile-app>. [Accessed: Feb. 2023].
- [13] "What is a Desktop App?," V2 Cloud, 2022. [Online]. Available: <https://v2cloud.com/glossary/what-is-a-desktop-app>. [Accessed: Feb. 2023].
- [14] "What is Internet of Things (IoT)?," Oracle, 2022. [Online]. Available: <https://www.oracle.com/internet-of-things/what-is-iot/>. [Accessed: Feb. 2023].
- [15] "What is HTTPS?," Cloudflare, 2022. [Online]. Available: <https://www.cloudflare.com/learning/ssl/what-is-https/>. [Accessed: Feb. 2023].
- [16] M. S. Al-Ruithe, R. A. Senousy and M. Hassan, "The Impacts of Demographics on Citizen Trust in the Adoption of E-Government," *Journal of Physics: Conference Series*, vol. 1362, no. 1, p. 012050, Dec. 2019. [Online]. Available: <https://iopscience.iop.org/article/10.1088/1742-6596/1362/1/012050>. [Accessed: Feb. 2023].
- [17] K. S. Sim, S. K. Tiong, J. S. Mandeep and C. P. Tan, "A secure electronic voting protocol for general elections," *Sensors*, vol. 21, no. 17, p. 5874, 2021. [Online]. Available: <https://doi.org/10.3390/s21175874>. [Accessed: Feb. 2023].
- [18] A. O. B. Alao and A. O. Adekunle, "Design and Implementation of Electronic Voting System," *ResearchGate*, Aug. 2017. [Online]. Available: [https://www.researchgate.net/publication/319176839\\_Design\\_and\\_Implementation\\_of\\_Electronic\\_Voting\\_System](https://www.researchgate.net/publication/319176839_Design_and_Implementation_of_Electronic_Voting_System). [Accessed: Feb. 2023].