Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

Smart Voting System by Using Iot

Mrs.P V Omkar, Annamdevula Prasanna Vijaya Lakshmi,
Tippanaboina S V Pavan Kalyan, Maddipoti Veerendranth Chowdary,
Arigi Vinod

Department of Electronics and Communication Engineering
Godavari Institute of Engineering and Technology(A), Rajahmundry, AP, INDIA.

ABSTRACT: **This project's Smart Voting System improves the security and effectiveness of conventional voting processes by utilising Python programming and Internet of Things-enabled embedded devices. Microcontrollers, biometric or smart card readers, push buttons or touchscreens, and Internet of Things communication modules are all integrated into the system to build a networked infrastructure that facilitates smooth communication between voters and a central server. Python is used for server-side programming, voter authentication management, real-time monitoring, and the safe database storage of voting data when combined with Flask or Django. In order to construct a dependable and trustworthy Smart Voting System, the offered code snippet provides a basic structure that guarantees one vote for each qualified voter and emphasises the significance of adhering to local rules and security standards.**

Keywords**: Arduino Mega 2560, Python, Embedded system, IOT, Sensors, Node MCU, ThingSpeak.**

INTRODUCTION

In this proposal, an online voting system based on Aadhar cards is proposed. The system uses the voter's fingerprint, which is stored in a central government database as their Aadhar card number. The government gathers biometric and demographic information from citizens in the Aadhar centralised database, which generates a 12-digit unique identity number for each person. Since each fingerprint is distinct from the other, fingerprint biometrics offer safe authentication.It also verifies an individual's age. Is the individual eligible to vote? If the individual is under eighteen (18 years old), they are not able to vote. In order to give its inhabitants better government, India is investing a large amount of money to upgrade its whole voting system. In India For a stronger democracy, the voting process should be transparent, free from corruption, and completely safe. Due to the possibility of tampering with votes during the voting process, the existing system is known for its lack of transparency. The three key issues of the current election voting process are voter authentication (uniqueness), voting process security, and voter data protection. We created our online voting system in order to overcome the difficulties. More security is provided by this system than by the previous one.

LITERATURE SURVEY

[1] Safe Electronic Polling Device Utilizing Biometric Technology with IOT, 2020 and Unique Identity Number In order to address problems like fraud and manual counting, the study presents a safe electronic voting system that integrates biometric face recognition, Aadhar ID, and IoT. It describes a two-step procedure for electronic voting and voter registration. It guarantees accurate face identification and recognition by employing the Haarcascade frontal face algorithm. Results from experiments in face spoofing, unauthorized, and allowed scenarios are presented along with comparisons with current technology, demonstrating lower error rates and increased accuracy. All things considered, the suggested system provides a strong way to improve voting efficiency and security.An Analysis of a Raspberry Pi-Based Face Recognition System for the Internet of Things Anima Sharma, Richa Sharma, and Arihant Kumar Jain (2018). The suggested solution uses IOT, Aadhar ID, and face recognition to provide a safe electronic voting technique. It transmits results immediately, authenticates voters, and counts votes automatically.

[2] An Examination of an Internet of Things Face Recognition System Based on a Raspberry Pi Anima Jain, Arihant Kumar, and Richa Sharma (2018).The study examines IoT and computer vision in home automation and security, and it suggests a face recognition system that makes use of Telegram and a Raspberry Pi. It covers algorithms, hardware/software components, and cites a number of scholarly works in the area.

[3] A review article on the use of Raspberry Pis for biometrics based on the internet of things Ingale, Trupti Rajendra, 2017.This study explores biometric techniques based on Internet of Things (IoT) and uses Raspberry Pi for fingerprint and face recognition. It assesses performance, security, and accuracy and talks about integrating cloud computing and IoT for authentication. It also surveys related works on face and fingerprint recognition on different platforms, with different algorithms and sensors.

[4] In order to simplify voting, an electronic voting machine (EVM) is introduced in the paper "A literature survey on micro-controller based smart electronic voting machine system" by S.V. Prasath and R. Mekala (2014). The EVM emphasizes speed, efficiency, dependability, and accuracy. Although it describes in depth the hardware and software of the EVM, the problem definition and purpose are unclear. It leaves out ethical, privacy, and security considerations and does not include a thorough literature evaluation. A comprehensive literature analysis, identifying research objectives, and addressing EVM obstacles are possible areas for improvement.

[5]. Premarket Sanjay Kumar Sing, "Use Fingerprint Technology to Create a Secure Electronic Voting System," International Journal of Computer ScienceIssues, Vol.10, No.4,2013. to create a safe electronic voting system with biometric fingerprint authentication that makes use of an Arduino Mega 2560 microcontroller, graphical LCD, keypad, SM630 fingerprint module, and Ethernet shield. The system seeks to reduce election expenses, increase reliability and transparency, remove fraudulent votes, and simplify operations by following established criteria for voting

EXISTING SYSTEM:

The Control Unit and the Balloting Unit are the two units that make up an EVM. The Ballot Unit is placed inside the democratic compartment, while the Control Unit is with the Presiding Officer or Polling Officer. The Polling Officer responsible for the Control Unit will press the

because the cycle is faster and more reliable. The surveying official is responsible for completing the genuine cycle of citizen recognition. Voters must present their Election Photo Identity Card (EPIC), which was issued by the Election Commission, in order for votes cast using electronic voting machines. When the surveying official compares the EPIC to the official breakdown he possesses, he must confirm that the card is authorized before allowing the citizens to project their votes. EVMs are therefore dependent on manual EPIC

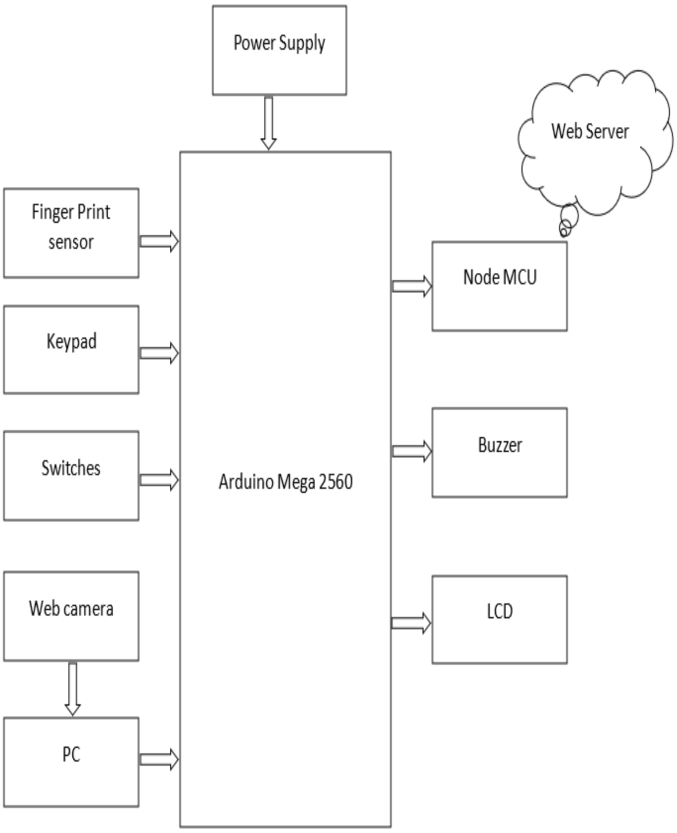

Fig.1.1 Proposed Block Diagram

Ballot Button instead of providing a voting form paper. By pushing the blue catch on the ballot unit, the voter will be able to project their vote against the rising star and the representation of their choice. At the moment of assembly, the working project of the silicon regulator used in EVMs is permanently damaged. Once the program is created, nobody can alter it. EVMs can accommodate up to 64 hard-charging newcomers.If there are more competitors than 16 in a BU, a second BU that corresponds to the primary BU will be connected. This setup is for only 16 up-and-comers in a BU. Similarly, if more than 32 applications are received overall, a third BU will be contacted; if more than 48 candidates are received overall, a fourth BU will be contacted, with a maximum of 64 applicants being considered. labor checks, which take more time. In this manner, EVMs depend on manual EPIC checks, which take more time.

DRAWBACKS OF EXISTING APPROACH:

- It consumes more time.
- And a man power is needed to take the count of voters and to identify the fraudulent voters.
- It requires manual verification of voter id each and every time.

PROPOSED SYSTEM:

The suggested intelligent voting system makes use of Internet of Things elements such as the ThingSpeak cloud integration, fingerprint sensor, webcam, keypad, buzzer, Arduino Mega, and NodeMCU. It seeks to improve security and transparency while streamlining the voting procedure. Together, the hardware parts confirm voters' identities and safely record their votes. Voters use the keypad to input their unique ID, which causes the system to start the biometric verification process. The webcam simultaneously takes pictures of faces in order to do facial recognition. Using biometric information that has been stored, the fingerprint sensor verifies voters' identities. The technology sends the data to the cloud platform and increases the vote total for the relevant party if the verification is successful. Real-time vote data monitoring and analysis are made possible by integration with ThingSpeak. Through the use of Internet of Things protocols, ThingSpeak and Arduino Mega or Node MCU may connect securely while transferring data. By storing, analyzing, and visualizing the voting data, the cloud platform improves voting accountability and transparency. Privacy and data security are crucial factors to take into account. To avoid unwanted access, biometric and face data are encrypted and safely saved on the PC. To prevent interception or tampering, data transfer between IoT devices and the cloud platform is encrypted. Reliability and scalability are important components of design. With redundancy and error-handling features, the system is built to support many voters at once and provide dependable operation under a variety of circumstances. Voter interaction is facilitated by an interface that is easy to use; it leads voters through the voting process and gives them feedback on the progress of their verification. By assuring the integrity of the data gathered and enhancing openness, efficiency, and security in the voting process, the technology increases public confidence in electoral systems

.

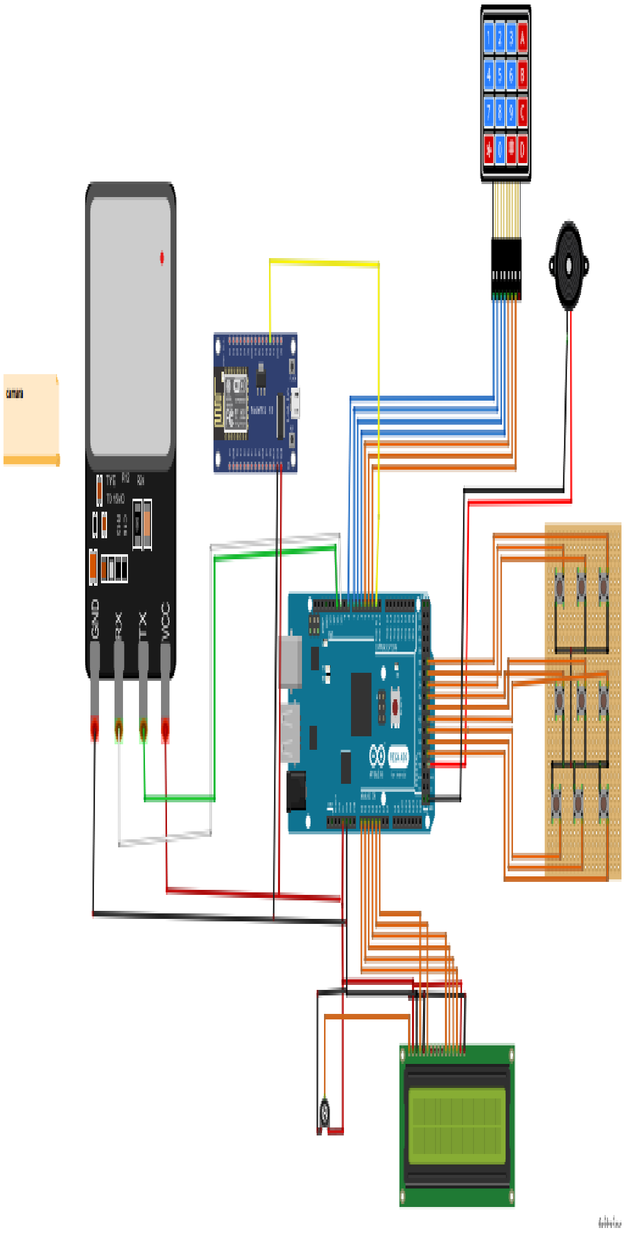

Fig.2.1 Circuit Diagram

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

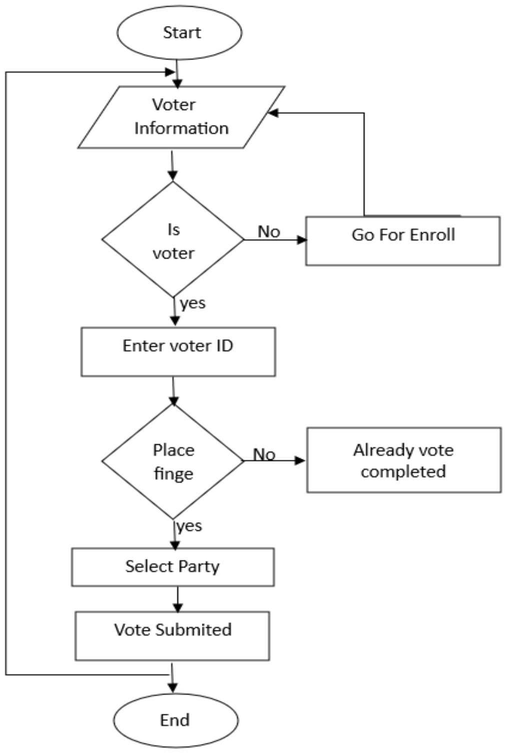

Fig.3.1 Flow Chart

REQUIRED COMPONENTS

A) HARDWARE REQUIREMENTS

1. ARDUINO MEGA 2560:

The Arduino Mega 2560 is a microcontroller board built around the ATmega2560 (datasheet). It includes 54 digital input/output pins (14 of which can be used as PWM outputs), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It includes everything necessary to support the microcontroller; simply connect it to a computer via USB cable or power it with an AC-to-DC adapter or battery to get started.

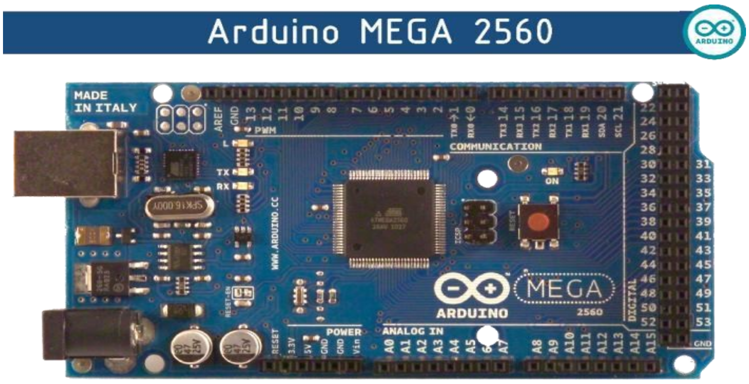

Fig.4.1 Diagram of Arduino Mega 2560

2. Finger Print Sensor

A fingerprint sensor is a type of biometric security equipment that takes a picture of a person's fingerprint and uses analysis to build a digital template by identifying specific characteristics. For authentication purposes, this template is then compared against saved templates. Smartphones, access control systems, and financial transactions all frequently employ fingerprint sensors for safe, convenient authentication that does not require passwords or PINs.

Fig.5.1 Diagram of Finger Print Sensor

3. NODE MCU :

Node MCU is an open-source firmware and development kit that helps you construct your own IoT product with just a few Lua script lines.The board features many GPIO pins for connecting with peripherals and supporting PWM, I2C, SPI, and UART serial communications. The module's interface is broken into two parts: firmware and hardware, with the former running on the ESP8266 Wi-Fi SoC and the latter based on the ESP12 module.

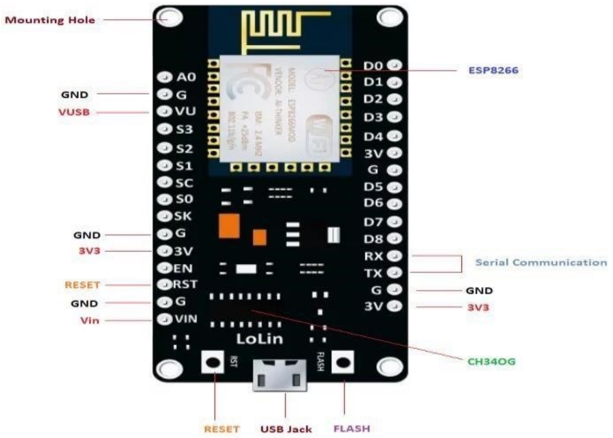

Fig.6.1 Diagram of Node MCU

4. Switches:

An electrical switch that is operated by pressing a button is called a pushbutton switch. It completes an electrical circuit when pressed, enabling current to flow. The circuit breaks when the release occurs. It is composed of terminals, an enclosure, metal contacts, and a button (actuator). There are two types of pushbutton switches: latching and momentary. Latching switches hold their state until they are manually turned back, while momentary switches return to their initial position when released. They serve as controls in a variety of electronic systems and devices..

Fig.7.1 Diagram of push button switches

5.Keypad :

An input device with buttons organized in a grid is called a keypad. A character, number, or function is represented by each button. By arranging these buttons in a matrix, fewer connections are required. In order to identify button presses, a controller scans the matrix. Keypads can communicate with devices in a number of ways. They are found in electronics like as industrial panels, security systems, and calculators, where they are utilized to input commands or data. Keypads offer users tactile input and are available in a variety of size sand combinations of the 3*4 keypad. .

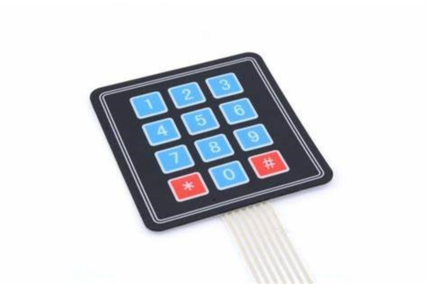

Fig.8.1 Diagram of 3*4 keypad

6.Liquid Crystal Display :

Electronic devices employ liquid crystal displays (LCDs), which are flat panels that provide visual data. Electric currents are used to regulate liquid crystal molecules, which in turn manipulates the properties of light. LCDs are available in multiple varieties, each possessing unique features such as TN, IPS, and VA. They are found in gadgets including calculators, smartphones, TVs, and displays. LCDs have certain benefits, such as low power consumption and support for various resolutions, but they can also have drawbacks, such as narrow viewing angles. They are generally adaptable and extensively utilized in contemporary electronics..

Fig.9.1 Diagram of Liquid crystal Display

7.Buzzer:

An electro-acoustic gadget known as a buzzer emits sound when an electric current flows through it. It is made up of a wire coil fastened to a piezoelectric element or diaphragm. A magnetic field is produced when current flows, which causes the diaphragm to shake and emit sound waves. There are many different kinds of buzzers, such as piezoelectric and electromagnetic ones, and they are used to provide auditory warnings or alerts in appliances, games, and alarm systems.

Fig.10.1 Diagram of Buzzer

B) SOFTWARE REQUIREMENTS

1. PYTHON IDLE:

Python's built-in integrated development environment is known as Python IDLE, or Integrated Development and Learning Environment. This feature-rich integrated development environment (IDE) simplifies Python program creation, execution, and debugging. Developers may run Python commands in an interactive shell inside IDLE, making it simple to test and explore. To enhance the scripting experience, IDLE includes a script editor with capabilities such as code completion and syntax highlighting. The inbuilt debugger aids in the discovery and resolution of issues by providing tools such as breakpoint setup and variable inspection during runtime. IDLE accommodates both novices and specialists by providing a built-in help system and file explorer for easy project navigation and quick access to Python documentation. While excellent for minor projects, more advanced IDEs such as PyCharm or Visual Studio Code may be preferred by some developers for more ambitious and challenging jobs.

.

2. ARDUINO IDE :

Arduino IDE (Integrated Development Environment) is an official program developed by Arduino.cc for creating, compiling, and uploading code to Arduino devices. Almost all Arduino modules are compatible with this open-source software, which can be installed and used to compile code while on the go.

3.THINGSPEAK :

ThingSpeak is an IoT analytics platform that allows you to collect, display, and analyze real-time data streams in the cloud. ThingSpeak enables you to send data from your devices, generate real-time graphs, and issue alerts. ThingSpeak is an open-source Ruby app that enables users to speak with internet-connected gadgets. It makes it easier to access, retrieve, and log data by giving an API to both devices and social networking websites.

RESULTS:

The Smart Voting System improves on conventional voting processes by combining Python programming with Internet of Things-enabled devices. Through the integration of biometric scanners, microcontrollers, and IoT communication modules, a safe infrastructure for voter interactions is established. Voter authentication, server-side programming, real-time monitoring, and data storage are all handled by Python in conjunction with Flask or Django. The system emphasises adherence to local laws and security requirements while guaranteeing one vote for each eligible voter over the age of 18. In general, the goal is to provide a dependable and trustworthy voting process.

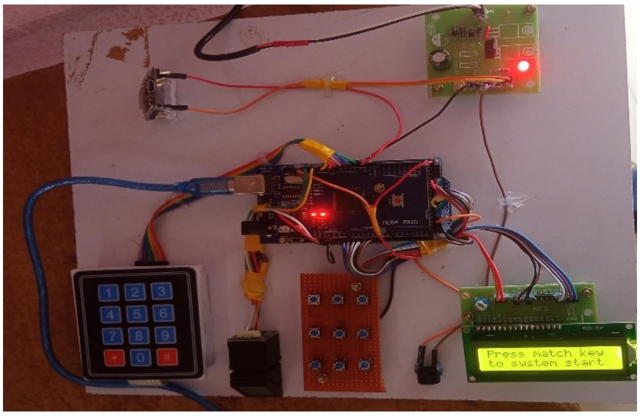

Fig.11.1 Final hardware implementation

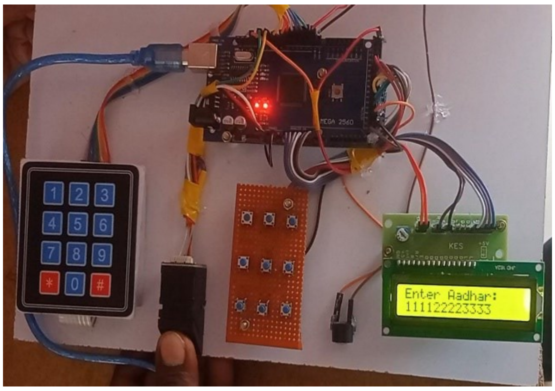

Fig.12.1 Enter the Aadhar Number and Displayed on

LCD

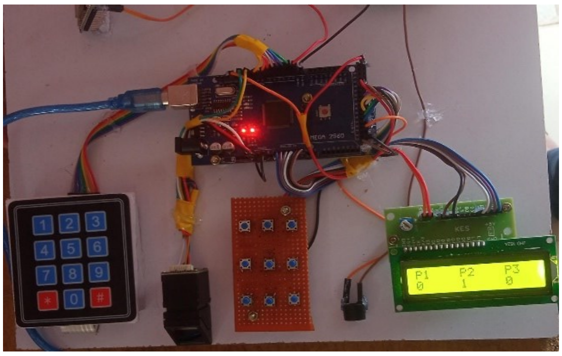

Fig.13.1 Output :Count of the votes

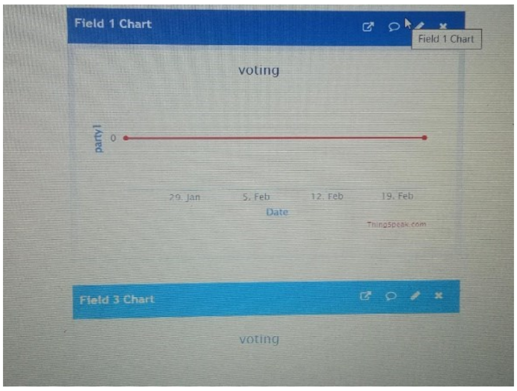

Fig.14.1 party-1 Count

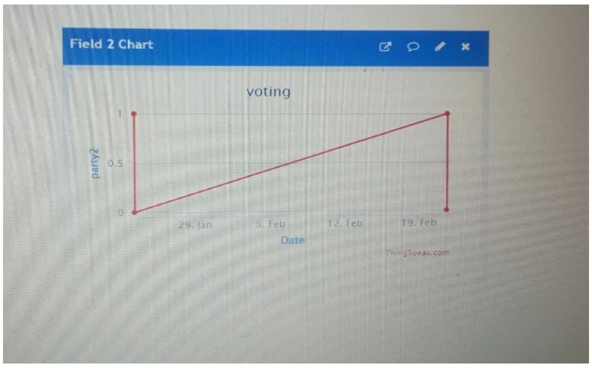

Fig.14.2 party-2 Count

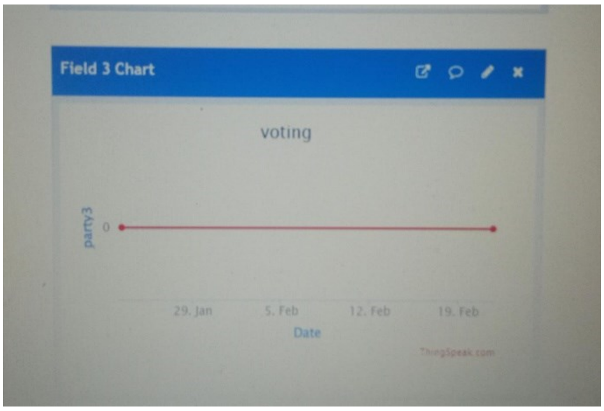

Fig.14.3 party-3 Count

FUTURESCOPE

The project to develop a smart voting system has a bright future ahead of it. Potential advancements include enhancing security with multi-factor authentication and blockchain, improving biometric recognition accuracy, and scaling the system for broader accessibility. Real-time monitoring and analytics could offer valuable insights, while remote voting capabilities may increase participation. Integration with government systems could streamline processes, and ongoing user experience enhancements would promote trust. Emerging technologies like AI, ML, and IoT could further automate and optimize the voting process. Overall, the project holds vast potential to transform electoral processes, bolster democracy, and ensure election integrity.

CONCLUSION

The smart voting system, integrating IoT elements like Arduino Mega, NodeMCU, fingerprint sensor, webcam, keypad, buzzer, and ThingSpeak cloud, ensures secure, efficient, and transparent voting. Arduino Mega and NodeMCU enable seamless hardware coordination, while biometric verification enhances security. Cloud integration enables real-time data storage and analysis. Overall, this system represents a significant advancement in electoral modernization, promoting inclusivity and safeguarding democratic integrity through IoT, biometrics, and cloud technologies.

REFERENCES

[1] Secured Electronic Voting Machine Using Biometric Technique with Unique Identity Number and IOT, 2020

[2] A Review of Face Recognition System Using Raspberry Pi in the Field of IoT Arihant Kumar Jain, Richa Sharma, Anima Sharma, 2018

[3] A Review paper on biometrics implementation based on internet of things using raspberry pi Trupti Rajendra Ingale, 2017

[4] A literature survey on micro-controller based smart electronic voting machine system S.V.Prasath, R.Mekala M.E. (Ph.D.), 2014

[5] P. S. Pandey, P. Ranjan, M. K. Aghwariya, "The Real-Time Hardware Design and Simulation of Thermoelectric Refrigerator System Based on Peltier Effect" ICICCD 2016 DOI 10.1007/978-981-10-1708-7_66, vol. 7, pp. 581- 589, (2016). International Journal on Human and Smart Device Interaction Vol. 2, No. 1 (2015) 6 Copyright ⓒ2015 GV School Publication.

[6] J.Ramprabu, G.Sindhuja "Performance Analysis of Open-Source Real Time Operating Systems" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue"

[7] IoT Based E-Voting System to Avoid Fraud Voting International Journal of Advanced Research in Science, Communication and Technology 28 Apr 2023

[8]Arduino Based Smart and Remote Voting System with SmartCard Implementation and Dual Biometric Authentication Suraj H P 31 Jul 2022-International Journal For Science Technology And Engineering

[9]Two Level Authentication for E-Voting System Using IoT Technology Swarnalatha M, Pooja Dharshini G, Castin Keerthana B, Nivetha R. P, Yazhini M, Sriman.S , International Journal of Advanced Research in Science, Communication and Technology 19 May 2022

[10]Blockchain and Internet of Things (IoT) Enabled Smart E-Voting System Durgesh Kumar, Rajendra Kumar Dwivedi
05 Jan 2023