Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**

GUARDIAN BALLOT: A SECURE IOT - BASED VOTING SYSTEM FOR FRAUD DETECTION

Ponnada Naga Sirisha[1]
sirishaponnada342@gmail.com

Doppa Sai Kumar[2]
saikumardoppa80085@gmail.com

Shaik Shahina Sulthana[3]
shaikshahinasultana5@gmail.com

Shaik Parvez Mohsin[4]
Parvezmohsin2002@gmail.com

Patnam Abhishek[5]
Abhispatnam@gmail.com

M Lenin Babu[6]
Hellolenin@gmail.com

Udatha Srinivas[7]
srinivas.Udatha@gmail.com

[1,2,3,4,5] *UG Students,* [6,7]*Assistant Professor,*
[1, 2, 3, 4, 5, 6,7] Dept. of ECE, Bapatla Engineering College, Bapatla
Andhra Pradesh, India

Abstract :

Modernizing and securing the electoral process is a pressing need in the digital age, where the integration of advanced technologies can significantly enhance the efficiency and reliability of voting systems. This project introduces an Arduino ESP32-based biometric voting system, leveraging the power of microcontroller technology to create a secure, user-friendly, and transparent voting experience. This project presents an Arduino ESP32-based biometric voting system designed to enhance the security and efficiency of the voting process. Integrating a camera for voter identification, a fingerprint module for authentication, and push buttons with LED indicators for real-time confirmation, the system ensures a secure and user-friendly voting experience. The admin interface provides instant access to voting results, contributing to transparent and accountable elections. This innovative solution aims to revolutionize traditional voting methods, ensuring the integrity and reliability of the democratic process. And also implementing the provisions which is helpful for blind people to appeal their vote . In the proposed system the results are also updated into the cloud storage.

Keywords: Arduino, mobile app, ESP32 Camera ;Wi-Fi Module; Fingerprint Sensor; LED Indicators, internet of things.

1 INTRODUCTION :

The ”Smart Voting System Using IOT” used to avoid Bogus voting and also it helpful for blind people to appeal their vote through some indicators. The project uses an Arduino UNO microcontroller to process voting in a secure way and the results are also updated into the cloud. After appealing their vote the result be visible on display and through the indicators like LED ,if green indicator is blinking with the buzzer sound it is successfully appealed their vote ,if red it might be a bogus vote. Simultaneously check the physically appeared person and the dataset which we already given as an input is correct or not.

1.1 Introduction To Modules

1. Fingerprint Sensor :

A fingerprint sensor can be integrated to ensure secure and accurate voter authentication. This sensor captures unique fingerprint patterns, which are then compared against a database to verify the identity of the voter before allowing them to cast their vote electronically. This adds an extra layer of security and helps prevent unauthorized access or fraudulent voting. Additionally, it enhances convenience for voters by eliminating the need for physical IDs or paperwork.

Fig. 1.1 (1). Fingerprint Sensor

2. ESP-32 Camera Module:

The ESP32-CAM is a small size, low power consumption camera module based on ESP32. It comes with an

OV2640 camera and an ESP32-CAM-MB micro USB to serial port adapter. The ESP32-CAM can be widely used in intelligent IoT applications such as wireless video monitoring, Wi-Fi image upload, QR identification, and so on. The ESP32 camera module can be integrated into a smart voting system using IoT to enable features such as remote monitoring of polling stations, facial recognition for voter authentication, and live streaming of voting processes. The module's capabilities, including its ability to capture images and video, coupled with the ESP32's built-in Wi-Fi connectivity, make it suitable for such applications. Additionally, data encryption and secure communication protocols should be implemented to ensure the integrity and confidentiality of the voting process.

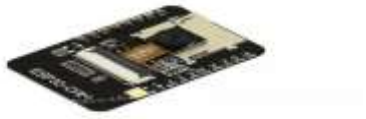

Fig.1.1 (2). Esp 32 Camera Module

3. Buzzer Module:

A buzzer module can be employed to provide audible feedback or alerts for various events during the voting process. This can include notifying voters when their vote has been successfully recorded, indicating the opening and closing of polling stations, or alerting election officials to any system errors or anomalies. The buzzer module can be controlled remotely via the IoT network, allowing for real-time updates and notifications. Additionally, the buzzer module can be integrated with other components of the system to enhance accessibility and provide a seamless voting experience for all users.

Fig.1.1 (3). Buzzer Module

4. LCD Display:

An LCD (Liquid Crystal Display) display can serve as a user interface to provide important information to voters and election officials. The LCD display can show instructions for voters, such as how to cast their vote, display the candidates' names and parties, and provide confirmation messages after a vote has been successfully cast.

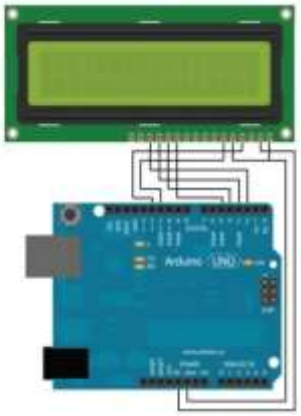

Fig.1.1 (4). LCD Display

5. ESP8266-01(Wi-Fi-Module):

Overall, the combination of a Wi-Fi module, fingerprint sensor, and camera module enhances the functionality, security, and transparency of a smart voting system using IoT technology.

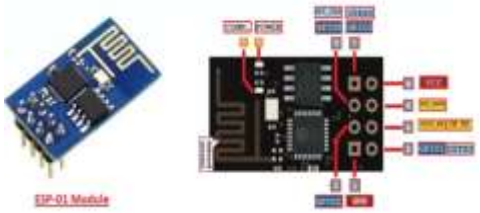

Fig.1.1 (5). Esp8266-01 (Wi-Fi-Module)

6 . Internet of Things:

The Internet of Things is known as IoT. IoT is difficult to define accurately. Expert in digital innovation, Kevin Ashton, has exploited the theme of IoT. And then it was really well liked.

The Internet of Things (IoT) is a network of interconnected devices that can exchange and collect data. Our essential appliances are integrated into a large number of digital devices via the Internet of Things.

With the advent of the Internet of Things, Smart voting system revolutionize traditional voting methods, ensuring the integrity and reliability of the democratic process. The physical world is merging with the internet of things to build one massive information system. IoT technology generates fresh concepts that improve the quality of our lives.

2 HARDWARE IMPLEMENTATION OF PROJECT :

2.1 *ARDUINO UNO:*

Arduino Uno is an open-source microcontroller board based on the Microchip ATmega328P microcon- troller, developed by Arduino.cc. It features 14 digital I/O pins and 6 analogue I/O pins, and can be powered via USB or an external 9-volt battery. The board is similar to

the Arduino Nano and Leonardo and is the first in a series of USB-based Arduino boards. The ATmega328 microcontroller on the board comes preprogrammed with a bootloader, allowing for easy code upload without the need for an external hardware programmer.

The Arduino IDE (Integrated Development Environment) software is compatible with Windows, MAC, or Linux systems, but Windows is preferred. Programming languages like C and C++ are used in IDEs. The Arduino Uno board can be powered by a USB cable or an AC-to-DC adapter, and it can be powered by Mirco SD cards for more information storage.

The board has a built-in regulation feature that keeps voltage under control when connected to an external device. A reset pin resets the board and takes the running program into the initial stage. The board has 13KB of flash memory for storing instructions in code. It requires 5 V to turn on, which can be achieved directly using a USB port or external adapter.

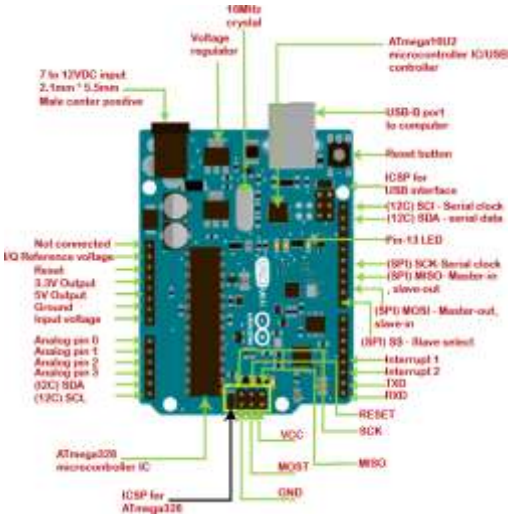

Figure 2.1: Arduino Uno Pinout

2.2 *Block Diagram:*

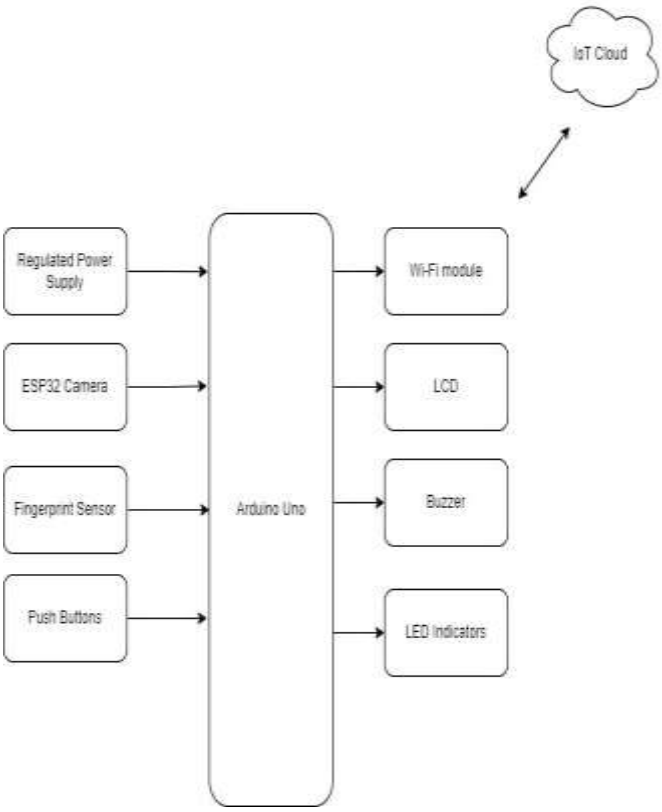

Fig 2.2 Block diagram

3 SOFTWARE

3.1 Arduino IDE:

The Arduino Integrated Development Environment (IDE) is a cross- platform application (for Windows, macOS, Linux) that is written in functions from C and C++. It is used to write and upload programs to Arduino compatible boards, but also, with the help of third-party cores, other vendor development boards. The source code for the IDE is released under the GNU General Public License, version 2. The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub main() into an executable cyclic executive program with the GNU toolchain, also included with the IDE distribution. The Arduino IDE employs the program avrdude to convert the executable code into a text file in hexa-decimal encoding that is loaded into the Arduino board by a loader program in the board's firmware. By default, avrdude is used as the uploading tool to flash the user code onto official Arduino boards. Arduino IDE is a derivative of the Processing IDE, however as of version 2.0, the Processing IDE will be replaced with the Visual Studio Code-based Eclipse Theia IDE framework. With the rising popularity of Arduino as a software platform, other vendors started to implement custom opensource compilers and tools (cores) that can build and upload sketches to other microcontrollers that are not supported by Arduino's official line of microcontrollers.

Fig 3.1. Arduino symbol

3.2 NODE-RED:

Node-RED is a flow-based development tool for visual programming developed originally by IBM for wiring together hardware devices, APIs and online services as part of the Internet of Things. Node- RED provides a web browser-based flow editor, which can be used to create JavaScript functions. Elements of applications can be saved or shared for re-use. The runtime is built on Node.js The flows created in Node-RED are stored using JSON. Since version 0.14, MQTT nodes can make properly configured TLS connections. In 2016, IBM contributed Node-RED as an open source JS Foundation project.

Figure 3.2 : Node Red

3.3 AWS Ec2 Cloud

The use of AWS EC2 cloud in a smart voting system leveraging IoT offers scalability, reliability, and security. EC2 instances can handle the computational demands of processing votes while IoT devices facilitate real-time data collection from polling stations. This architecture ensures efficient and secure voting processes, enhancing transparency and accessibility in elections.

Figure 3.3 : AWS Cloud

4 IMPLEMENTATION:

A prototype of our suggested method has been created and is tested in our lab to look at its architecture. There are primarily two sections to the implementation phase. The hardware component is one, while the software component is another. The following is a detailed description of the implementation phase:

4.1 *WORKING* :

In this project we have used Fingerprint Sensor, camera module, Wi-Fi module, LCD display, Arduino Uno Micro- controller and IOT Cloud, buzzer sensor, LED indicators. Basically its is a IoT based project. Our main moto of this project is to detect the fraud voting i.e Bogus voting and also helpful for blind people to cast their vote.

Firstly we implement the code. With that code we give a dataset as an input. In that dataset, there is an information namely, voter ID, voter name, fingerprint details, face details (voter picture). These are all happening on software section. Upload upto 5 to 6 member details on the dataset. For example: A,B,C,D,E are the voters in a particular village who are used to cast their vote.

When person A comes to the polling booth, our kit scans face through camera module & fingerprint through respective sensor. When he going to appeal their vote, our kit simultaneously check the physically appeared person and the above mentioned dataset details are matched or not.

CASE 1: If it matches, the voter A is going to appeal their vote, after completion of voting , a buzzer sound be heard and a green bulb is blinking like an indicator of successful completion of voter A in specified region be displayed on LCD display. Through this process we avoid bogus votes or fraud votes. Likewise voter B,C,D are appealed their vote.

Here if voter E is missed to cast their vote, at final wee show that the count that how many members are appealed their vote. For example voter A,B,C,D are appealed then display count 4 appealed, voter E are missed then display count 1 not appealed.

CASE 2: If it doesn't match then the voter is not in the list. For example voter X be come to the polling booth and appealed their vote, Red bulb indication be given.

After completion of all the voting process the data be stored into cloud. Results be displayed i..e parties classification can also be taken place. For example voters A & B –TDP,C & D— Janasena , E—YSRCP.

This classification or the result must be accessed by a specific person(example :our project guide).Through the guide fingerprint only the result be accessed or opened. We are adding some provisions /components which is helpful for blind people to cast their vote. For example: Braille

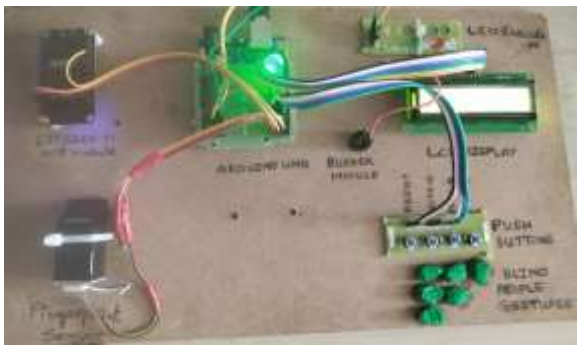

Figure 4.1 : kit connection

5. FUTURE SCOPE :

5.1 Use cases:

This is designed to detect the bogus voting in voting process and also it is more flexible for blind people to cast their vote. This innovative solution aims to revolutionize traditional voting methods, ensuring the integrity and reliability of the democratic process. In the proposed system the results are also updated into the cloud storage.

5.2 Dependency:

We are not willing to terminate our project as prototype. but, make our project to be in the real time market to replace the traditional methods to avoid fraud voting. For that, still economical support and technical support from experts is required.

5.3 Future development:

We can add a “Remote Voting” enabled devices such as smartphones or tablets can be used for remote voting, allowing voters to securely cast their ballots from anywhere. Biometric authentication and blockchain technology can be utilized to ensure the integrity and security of remote voting processes. And second one is “Feedback Mechanisms” enabled feedback devices can be deployed at polling stations to gather feedback from voters about their voting experience. This information can be used to identify areas for improvement and make necessary adjustments to enhance voter satisfaction.

6. Results :

In this project, we presented the obtained results from the application of the proposed system of hardware, firmware and android application which is implemented using IoT technology.

Fig 6.1 party A voting result

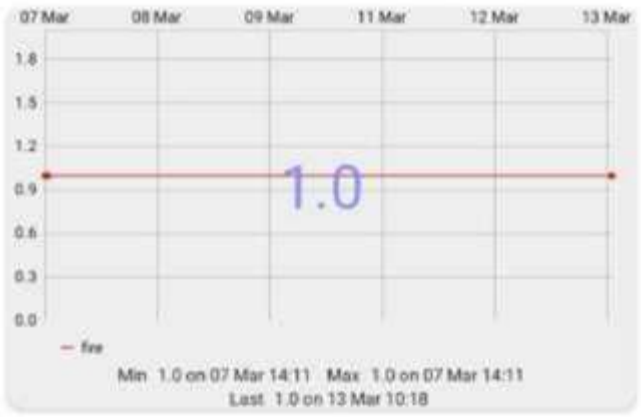

Fig 6.2 party B voting result

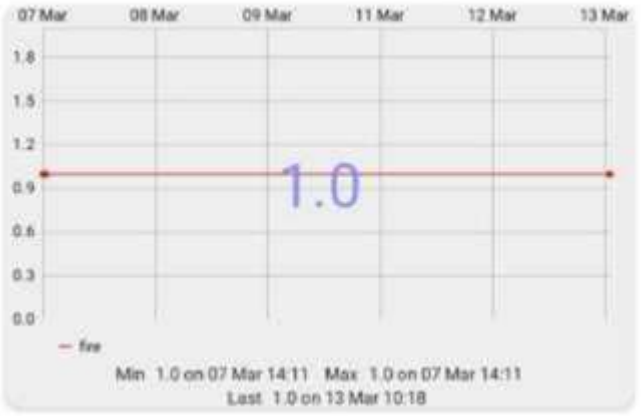

Fig 6.3 party C voting result

7. Conclusion :

The proposed system will provide an innovative solution aims to revolutionize traditional voting methods, ensuring the integrity and reliability of the democratic process, and it is secure, user-friendly, and transparent voting experiences, and also it is helpful for blind people to appeal their vote without help of other person. The results are also updated into the cloud storage.

8. References:

1.Design of an Internet of Things (IoT) Based Secure Electronic Voting System" by Vivek Ashok Bohara and Akshaykumar Patel, in the International Journal of Computer Applications (IJCA), 2017.

2."Development of Smart Voting System Using Internet of Things (IoT)" by P. Ramaiah and B. Venkateswarlu, in the International Journal of Engineering Research and Applications (IJERA), 2018.

3."IoT Based Secure Electronic Voting System Using Arduino" by G. Sivaraman and R. Abarna, in the International Journal of Pure and Applied Mathematics (IJPAM), 2019.

4."Smart Voting System Using IoT and Blockchain" by M. Vijayalakshmi, V. Muthukumaravel, and M.

Sakthivel, in the International Journal of Engineering Research & Technology (IJERT), 2020.

5."An IoT Based Secure and Reliable Voting System" by Sandeep Saini, Shubham Saini, and Bharat Bhushan, in the International Journal of Computer Science and Information Technologies (IJCSIT), 2018.

6."Smart Voting System Using IoT and Blockchain Technology" by R. Harshitha, R. Mounika, and T. Shobha Rani, in the International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 2019.

7."Design and Implementation of a Secure Internet of Things (IoT)-Based Electronic Voting System" by James Ubong, Samuel Idowu, and Stanley Tochukwu Eze, in the Journal of Information Security, 2020.