Disinfected Smart Voting System using Aadhaar as UID

Praveen Kumar K[a], Sitesh Kumar Sinha[b], and Shivamurthaiah M[c]

[a]
Research Scholar, Dept. Computer Science and Engineering
Rabindranath Tagore University, Bhopal, India
[b]Professor, Dept. Computer Science and Engineering
Rabindranath Tagore University, Bhopal, India
[c]Assistant Professor, Bengaluru

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: The election is the central criterion in every country to choose their best leader in society. Meanwhile, the technologies used in the time of the election are also an important thing to maintain the economic balance, security for the voting, and safety of the voter's health as well. Currently in India, we are going to use the EVM machines to cast the votes, this method of manually maintaining the process of the election is a tedious task, for this, we are going to introduce a system of maintaining the election procedure electronically by using the IoT device with Aadhaar linking called Biometric with automatic sanitization of the voters during the time of the election with giving the security to the casted votes in the central hub safely. The method of linking the Aadhaar data to the election is to avoid the proxy voters during the time of the election, introducing the IoT device of the automated sanitizing device in the polling station may help to avoid the spreading of the pandemic from the biometric device. The maintaining of the security of the votes carried out by using the MAC address.

1. Introduction

The election is of the leading procedural to choose the leader in the country, every country has its electoral procedure for the election. India is one of the biggest countries by following the rules of the constitution. In India nowadays the concept of the making of India like Digitalization can proceed. During this, the Aadhaar linking to every sector is a method of making the identity for every citizen in the country. As well as in the present era technology improves, more and more using the automation and maintaining every process is through the online may reduce the manual process and avoiding all most all the proxy in every sector. Regarding these aspects, IoT is a concept of improving the atomization of the systems in every sector. By using these IoT concepts we are proposing a system of online voting. Our application consisting of the Aadhaar based voting system from their present place rather than moving to their native constituency. Moreover, this application concentrating on the system of an epidemic that occurs from the biometric device during the time of the election by introducing the temperature sensing device with the automated sanitizing device. Along with the IoT concept of the biometric device, by introducing the MAC [Media Access Control] binding system for saving the data (votes) from the unauthorized people while sending the votes from the polling stations to the main server.

This application tackles the Aadhaar database with a temperature sensor along with an automated sanitizing device and MAC binding concept to save the data.

When the election officers enter to any polling station for further more inquiries he must log in to the application to save the location of the every individual booth, these locations are saved in the application safely, when the election officer enters to the booth to make further more arrangement the location must be matched with the previously saved location, by using the system of GPS location.

Basic functionalities needed in the voting in our application

1. People must be enrolled with the Aadhaar card.
2. The Aadhaar based voting site should be accessible at the voting booth.
3. Fingerprint scanner should be provided at the voting booth.
4. Internet and Electricity should be required.

About Biometric, Fingerprint, and Aadhaar

One of the method to identification of every individual is based on the physical, chemical, or behavioural characters of the person. This can include fingerprint, face, iris, retina, signature, gait, palm print, voice pattern, ear hand vein, etc., info of an specific to create identity. This info is unique to every person.

From the many decades people have used the fingerprint for personal identification. Identification of the human by fingerprint results high accuracy. Even the persons fingerprint of identical twins are also different. In the present system the fingerprint scanner cost is less than 5000, so it is reasonable for the purpose of authentication**.**

Recently Indian government make the plan of Unique Identification Authority of India (UIDAI) created and Aadhaar card. In the Aadhaar database government collects the biometric and demographic data of the people, and store them in a centralized database, and issued a 12-digit unique identity number to each persons and it will not same for any of those enrolled to the Aadhaar. It has to be considered the world’s largest national unique identification number.

Existing Voting System

Electronic Voting Machine(EVM) are replaced from the year of 1998 in India. The EVM consisting of the two units called Control and Balloting units. These two units are connected to the five meter cable. The control unit is present with the Polling Officer and therefore the Balloting Unit is located inside the voting compartment. Instead of providing a ballot paper, the Polling Officer can press the Ballot Button. Rather than issuing a ballot paper. This will allow the voter to cast his vote through pressing the blue button on the voting unit symbol of his choice.

Problems of Present voting system:

People who stay away from their native constituency will not cast the vote on the day of election:

The students of the age group 18-25 are studying in colleges. If the students of this age grouped stayed away from their native for the studies would'nt ready to spend thousands of rupees for the purpose of voting. Similarly many people of the age group 25-40 are working in places thousands of kilometers from their homes. From where they are not able to come home on Holi, Diwali. How can we expect they come and cast a vote? And that's why the voting percentage is low.

Illegal Voting: The very commonly known problem is Illegal voting, which is faced in every election. One person casts the votes of all the members or few amounts of members in the listed as illegally. This results in the loss of votes for the other candidates participating and also increases the amount of votes to the candidate who performs this action. This can be done externally at the time of voting.

The existing EVM's elections systems were done using the ballot, ink, and tallying the votes later. But our proposed system offers the election accurately.

Proposed System

By using the internet, we can easily get the vote of the people using the aadhaar database. Aadhaar based Election Voting System

Steps involved in the process

3.1 Steps implemented in the System:

Step 1: Enter to any polling station in the State.

Step 2: Then after your turn goes into the voting compartment.

Step 3: Place the finger in the device

Step4: The automated temperature sensor will sense the human body temperature, and displayed it on the screen of the election officer.

Step 5: Then the system automated sanitizing device will dispense the sanitizer for his hand.

Step 6: The person enters his fingerprint to a scanner.

Step 7: The system checks fingerprint with the Aadhaar database's fingerprint and also checks the are eligibility of the persons regarding voting(age 18 or not).

Step 8: Then if you are eligible then it shows the message "You can vote" or else it shows "Your not eligible to vote"

Step 9: The person's details will show to the election officer in the polling station then after seeing the information of the citizen, he can have the options to accept or reject the person. After accepting from the officer.

Step 10: You can reach the other screen of the booth and then you can choose the candidate from the list of candidates.

Step 11: Then the vote is successfully stored.

The methods involved in the process

1. Automated sanitizing device for biometric

During the time of the election using a biometric device for identifying the authorized person using the Aadhaar database may be a good process, the question is, to avoid the pandemic by using the same device at the time of the election. For this problem, we are going to propose a system of automatic sanitization methods. Regarding this, the concept of the IoT device is introduced to automate the system. The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [1,2,3].

By using the physical device like biometric, during the time of the election is a process. There is a problem with a pandemic by using the same device for all the people. Pandemics are large-scale outbreaks of infectious diseases that can greatly increase morbidity and mortality over a wide geographic area and cause significant economic, social, and political disruption. Evidence suggests that the likelihood of pandemics has increased over the past century because of increased global travel and integration, urbanization, changes in land use, and greater exploitation of the natural environment.

To avoid this problem the automated sanitizing device with biometric can be introduced in this system.

The device contains the first phase, which is used to identify the body temperature of the person to know about his health condition regarding the fever. When the person enters to the polling station, they must place their hand in the unit of the device, then it measures the body temperature of the person and it will display on the screen which is connected to the booth officer. If the temperature is high the device sounds the beep sound. After the measurement of the temperature, the sanitizer will be dispensed after a few seconds. After the completion of the sanitizing the second unit of the device will be opened to make the fingerprint [4, 5, 6]. The person who is using the sanitizer to his hand can wait until the next shutter is opened, after the 30 seconds the shutter will be opened and it will go to allow the person to enter the fingerprint which is connected to the main server.

By using the automated sanitizing method for the device may clear the confection of the people about the pandemic from the fingerprint device during casting the votes. This method is implemented by keeping things in the mind of maintaining health also.

Basic methods used in the device:

The device is integrated with the IR sensor, Microcontroller, and Thermal sensor

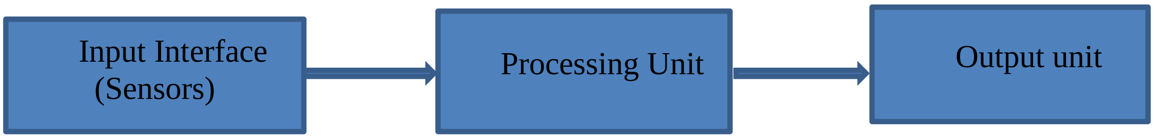
When the person places his hand to the unit of the IR sensor it will going to be sends the signals to the microcontroller in the device [IR sensor is used as the obstacle sensor], the microcontroller then sends the signals to the thermal sensor which is integrated to the device this thermal sensor can take the readings of the temperature of the human body and sends the readings to the microcontroller again.

Algorithm for the system:

```
Statement-1  Read Human_Body_Temperature (Using temperature sensor)
If human_body_temperature greater than the normal body temperature Then
Statement-2  Sanitizer dispensed //for 3 seconds//
Statement-3  Wait//15 seconds//
Statement-4  Shutter opened
Statement-5  Read user fingerprint
If    User fingerprint is equal to Aadhaar fingerprint Then
Statement-6 Accept for voting
Else
Statement-7 Reject for voting's
Else
Statement-8 Beep sound
        Sanitizer dispensed
Exit
End If
```

Basic Components of a System

The device can be divided into three basic components



Input Interface

It is the first unit of the system and called as sensitive component of the system that is used as an obstacle sensor that recognizes the human hand and sends the signals to a microcontroller that is present in the processing unit.

Processing Unit

The processing unit is a microcontroller. It activates the thermal sensor for knowing the temperature of the human body using their hands and that processes the data captured from the sensors.

Output Unit

The Output interface is the final unit of the system, which communicates with decision of the system to enable access to the user. This can be a simple sequential communication protocol or one of the many cellular protocols.

Terminologies of the Device:

IR Sensor: Which senses the human hand and sends the signals to the microcontroller.

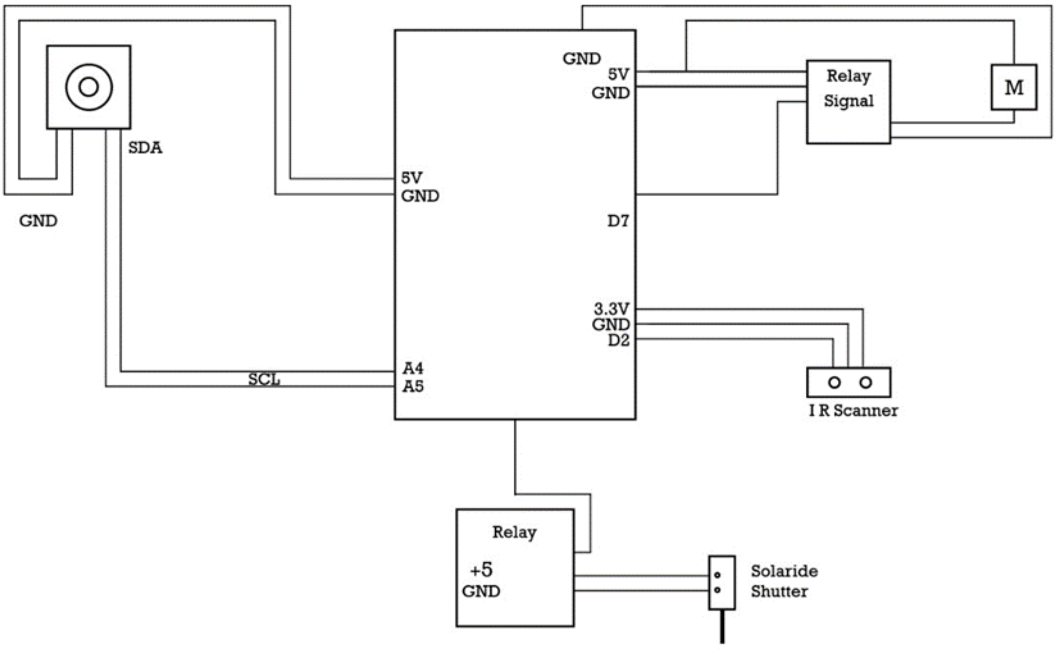
Microcontroller: Which activates the thermal sensor and working as a logical unit

Thermal Sensor: Taking the readings from the human hand and sends those data to the microcontroller.

Candidate/Subject − A person who enters his hand as a sample.

Task – 1. Identifying the human body temperature
2. Automated sanitizer
3. The shutter will be open for biometric
4. A beep sound will be held if the temperature is greater than the assigned temperature.

After opening the shutter the person will allow making the fingerprint using the Biometric Device



Block Diagram of the Working Model

General Working of a Biometric System

There are four general steps a biometric system takes to perform identification and verification −

1. Obtain a live sample from the candidate. (Using sensors)
2. Extract prominent features from the sample. (Using processing unit)
3. Compare live samples with samples stored in the database. (Using algorithms)
4. Present the decision. (Accept or reject the candidate.)

The biometric sample is acquired from the user. The prominent features are extracted from the sample and it is then compared with all the samples stored in the database. When the input sample matches one of the samples in the database, the biometric system allows the person to access the resources, otherwise prohibits.

2. Security measures of voting

Giving the security of online based voting is the main thing while at the same time making the digitalization of the internet casting a ballot framework. There might be an opportunity of losing information. Because of this, we are acquainting VPN security with this application [7, 8, 9].

The idea of saving the information from the unapproved people is MAC (Media Access Control) Binding, While doing this all the mentioned customer frameworks are associated the primary worker which is taken care of by the administrator of the application, when all the mentioned customer frameworks send the information to the worker framework it will just acknowledge the customers' framework information which have been now educated with the specific MAC address, this strategy for restricting the Mac address assists with getting to the information from the unauthprised people and sending the information from the other unauthprised addresses.

Methods involving online security in our application:

A firewall is an organization security gadget that screens approaching and active organization traffic and concludes whether to permit or obstruct explicit traffic dependent on a characterized set of security rules. Firewalls have been the principal line of safeguard in network security.

Data packets traveling the Internet are transported in cleartext. Consequently, anyone who can see Internet traffic can also read the data contained in the packets. While sending the votes from the client system using the internet. VPNs overcome these obstacles by using a strategy called tunneling. Instead of packets crossing the Internet out in the open, data packets are first encrypted for security, and then encapsulated in a Mac package by the VPN and tunneled through the Internet. The site to site VPN is used in this application for the most convenient method to save the data.

The site to Site VPNs:

A site-to-site VPN permits branches in different fixed areas to set up secure associations with one another over a public organization like the Internet. Site-to-site VPN broadens the network, making computer resources from one location available to the client system at other locations.

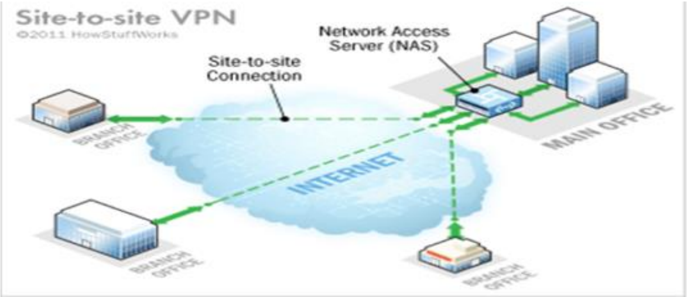


Fig 2: Site to site VPN

A single private network, they can create an intranet VPN to connect each separate LAN to a single WAN. Extranet-based – The extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate intranets.

Components to Establish/Setup VPN: 1. Authentication 2. Tunneling 3. Encryption

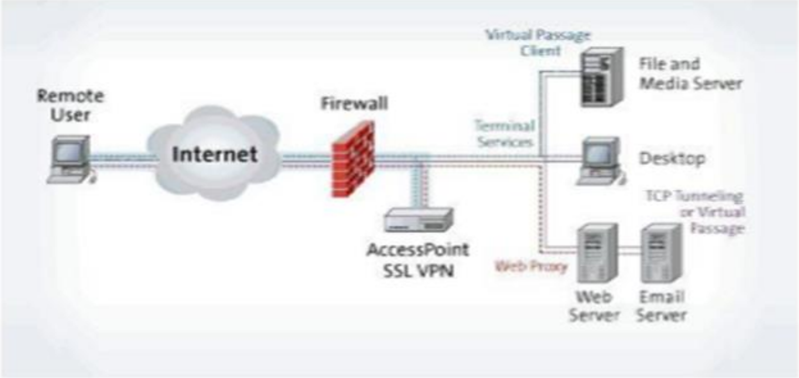
1. Authentication: Tunnel endpoints should be validated before secure VPN passages can be set up. Client made distant access VPNs may utilize passwords, biometrics, two-factor verification, or other cryptographic techniques. Network-to-network tunnels often use passwords or digital certificates. They permanently store the key to allow the tunnel to establish automatically, without intervention from the user.

.2. Tunneling: The VPN technology is concerned on the idea of the tunneling.It involves establishing and maintaining a logical network connection(that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side. Point-to-Point Tunneling Protocol (PPTP) is used to build the connection because nearly all flavors of Windows include built-in client support for this protocol.

3. Encryption: After the VPN connection is made we are using MAC Sec to create a secure connection to get end to end data encryption

Mac address:

Every device has a MAC address, a hardware identification number that is unique to it. While accessing the application, every device is assigned as a web URL. This forces a particular device to access the application from a specific URL. If either the MAC address or the web address changes, the device will not be able to access the application. MAC-binding will also enable authorities to trace a device based on its online activity.



Advantages of VPN

- There are two main advantages of VPN’s, namely, cost-saving and scalability.
- VPN’s lower costs by eliminating the need for expensive long-distance leased lines.
- A local leased line or even broadband connection is all that’s needed to connect the internet and utilize the public network to surely tunnel a private connection.
- Data transfers are encrypted.
- The cost is low to implement.

The process involved in the proposed model

Step 1: Start.
Step 2: Get MAC.
Step 3: Any request from the client.
Step 4: Server check and respond.
Step 5: If the bind is not matched, the server has not accepted the data.
Step 6: If the binding match also server will respond to the client (accept the data).
Step 7: Exit.

Advantages of the proposed system

1. Citizens can vote from their present place for their home constituency.

2. Illegal voting will be removed because of Fingerprint (a biometric is unique to each individual).

3. Aadhar's database permits only eligible voters to cast vote and, it also ensures that eligible voters vote only once.

4. It increases the voting percentage[10].

5. This method of approaching saves the time and money for traveling.

6. Quick results are possible [11,12].

Conclusion

This system provides the btter solutions to problems related to the present voting system of Indian voting system. This system helps to increase the voting percentage. In this voting process authentication can be done using biometric recognition to cast voter's votes, it ensures that vote casting cannot be altered by an unauthorized person. It requires a Computer/ Touch screen computer, Fingerprint scanner, and electricity. It also concentrates on the security of the votes along with the health of the citizens during casting the votes. The online-based voting system helps to avoid the manual system and the security measures using in this application may save the data.

References

1. Online Voting System using Aadhaar Number With OTP, ISSN:2393-9028(Print)|ISSN:2348-2281(online), IJRECE Vol.7 ISSUE 1(JANUARY-MARCH 2019) Praveen Kumar K1, Sitesh Kumar Sinha2, Shivamurthaiah M3 Department of Computer Science and Engineering, Rabindranath Tagore University, Bhopal M P
2. Prof.R.L.Gaike, Vishnu P. Lokhande, Shubham T. Jadhav and Prasad N. Paulbudhe, Aadhar Based Electronic Voting
3. Design a Secure Electronic Voting System Using Fingerprint Technique, ISSN 1694-0784, Volume-10, Issue -4, and IJCSI.
4. The Design And Development of Real-Time E-Voting System In Nigeria With Emphasis On Security And Result Veracity ,I.J. Computer Network and Information Security,2013,5,9-18,MECS.
5. The Design of Web Based Secure Internet Voting for Corporate Election, ISSN 2319-7064, Volume-2, Issue-7, July- 2013, and IJSR. International Journal of Engineering Research and General Science Volume 3, Issue 2, March April, 2015 ISSN 2091-2730 1118 www.ijergs.org
6. Frances Zelazny proposed the UIDAI, Biometrics Design Standards for UID Applications, 2009
7. Khasawneh, M., Malkawi, M., & Al-Jarrah, O. (2008). A Biometric-Secure e-Voting System for Election Process. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan.
8. Neha Gandhi, "Study on the security of online voting system using biometric and stenography" International journal of computer science and communication, Volume 5.
9. Sweta A. Tambe, P. S. Topannavar, "The Stenography And Biometric Online Voting System" International Journal of Advanced Research of Computer Science and Software Engineering, Volume 5, [ISSN-2277128X]
10. Biometric fingerprint based electronic voting system for rigging free governance using ARM7 TDMI processor based LPC2148 controller, K.Mallikarjuna1, T.Mallikarjuna2, INTERNATIONAL JOURNAL OF ENGINEERING & SCIENCE RESEARCH (IJESR/May 2014/ Vol-4/Issue-5/410-414) e-ISSN 2277-2685, p-ISSN 2320-976
11. Fingerprint Based e-Voting System using Aadhaar Database, Rohan Patel1, Vaibhav Ghorpade2, Vinay Jain3, and Mansi Kambli4, INTERNATIONAL JOURNAL FOR RESEARCH IN EMERGING SCIENCE AND TECHNOLOGY, (Volume-2, Issue-3, March-2015) E-ISSN: 2349-7610
12. Fingerprint and RFID Based Electronic Voting System Linked With AADHAAR for Rigging Free Elections, B.Mary Havilah Haque1, G.M.Owais Ahmed2, D.Sukruthi3, K.Venu Gopal Achary4, C.Mahendra Naidu5 INTERNATIONAL JOURNAL OF

ADVANCED RESEARCH IN ELECTRICAL, ELECTRONICS AND INSTRUMENTATION ENGINEERING (Vol. 5, Issue 3, March 2016) ISSN (Print): 2320 – 3765, ISSN (Online): 2278 – 8875