| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

Development of Online Voting System Using Aadhar Authentication

Chetan Adhikari[1], K.B.Ramesh[2], Ayush Upadhyay[3], Karthik Akasaligar[4]

UG Student, Department of Electronics and Instrumentation Engineering, RV College of Engineering, Bengaluru, India[1]

Associate Professor, Department of Electronics and Instrumentation Engineering, RV College of Engineering, Bengaluru, India[2]

UG Student, Department of Electronics and Instrumentation Engineering, RV College of Engineering, Bengaluru, India[3]

UG Student, Department of Electronics and Instrumentation Engineering, RV College of Engineering, Bengaluru, India[4]

ABSTRACT : In a country like India which is the world's biggest democracy, the electing of the leaders is one of the fundamental rights of each citizen. Recently the government has made providing eVoting facility to creditors compulsory under the Insolvency and Bankruptcy Code 2016.This proves that Government of India appreciates that online voting is important for the protection of 'right to vote' of people. But as India is a developing country it faces many risks to the security and the transparency to which each vote is cast. Seventy percent of the population of India belong to the rural background and each vote cast by them is precious and mustn't be not be influenced by external factors other than the voter himself. But sadly many of the times we observe that there are high chances of false votes, threatening of the voters and many other such malpractices. In order to eradicate such practices a safe and secure voting system must be established so that each vote is valid and the individual rights of the voters is protected. By developing an online voting system using Aadhaar authentication we aim to develop a secure system which is linkedwith Aadhaar card for accessing fingerprint biometric identification. This system enhances the security which is the need of the voting system. The problem of voting is still critical in terms of safety and security. This paper deals with the design and development of a web-based voting system using cloud computing and Aadhaar card in order to provide a high performance with high security to the voting system. We also use web technology to make the voting system practical. This system that has been introduced make sure before the vote has been casted the voter id and other credentials are checked like biometric. Most importantly the aadhar details are verified on the server and give the system utmost confidence that the voter isn't a fake person but in fact genuine. This kind of system wherein the voters identity is verified using the aadhar details increases transparency and reduces the possibility of false votes.

KEYWORDS: cloud computing Aadhaar, biometric identification

I.INTRODUCTION

The current system is the online voting system with authentication using Aadhaar card. As an input to the system the voter has to give his Aadhar details and biometric to the server and the fingerprint scanner respectively. The scanning is further processed by the matlab device. The Aadhar details are further collected by the UAI and stored on their server. Part of these details are then transferred to our cloud server for maximum security. The microcontroller and the fingerprint scanner constitute the internal and external hardware of the system respectively. The cloud server is also connected to the web and the gsm module for the output of data which is used to portray the tabulation of the poll results either as an SMS or in webpage format. As we see above the voting system is very secure and transparent hence it minimizes the chance of violence in the system and many other such malpractices. Also the servers can be accessed by only certified professionals hence no one can breach the security system.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

A.Objectives

1. This is a voting system by which any voter can vote from anywhere in the country.
2. Security is number one priority.
3. Increase percentage of votes from the rural background and decrease false votes.
4. Time is no longer a factor and mass updates cannot change the system overall and hence minimizing the chance of malpractices.

B.Literature Survey

In Secure Authentication for Online Voting System uses PIN, biometric images and stenography for authentication. Hash code is used to check if stenographic image is tampered or not. Pixel selection algorithm used will make PIN retrieval impossible. In Aadhaar Based Electronic Voting System using Fingerprint and Hex keypad has been designed successfully. Database consisting of the personal details should be updated every time before election. It is very difficult to design an ideal E-Voting system which allow perfect security and privacy with no compromise. In Fingerprint and RFID Based Electronic Voting System Linked with Aadhaar provide a security with RFID based Biometric voting method. And provides safety from alcoholic person whose comes to polling booth. This system interlinked with primary specification such as Voter ID, Aadhaar ID and Biometric authentication. There is no scope to take place ragging in Election. In Implementation of Authenticated and Secure Online Voting System helps in achieving the authenticity, Non-traceability of vote cast and security with confidentiality also being enforced. It provides secure voting password at the time of the registration which enables the voter to securely cast their vote along with biometric identification.

C.Research gap

1. There is increasingly widespread adoption of Direct Recording Electronic – DRE voting systems. DRE system completely eliminates paper ballots from the voting process.
2. The most fundamental problem with such system is that entire election things on the correctness and software installed within each of the voting terminal.
3. An Electronic Voting system is a voting system in which the election data is recorded and processed as digital information. E-voting is referred as “Electronic voting”. E-voting is an election system that allows a voter to record their ballots in an electrically secure system.
4. The main drawback of this system that it encounters the non- availability

II.METHODOLOGY

A. Block diagram

The methodology to achieve the objectives of this project is obtained by the block diagram as shown in the fig 2.1.1

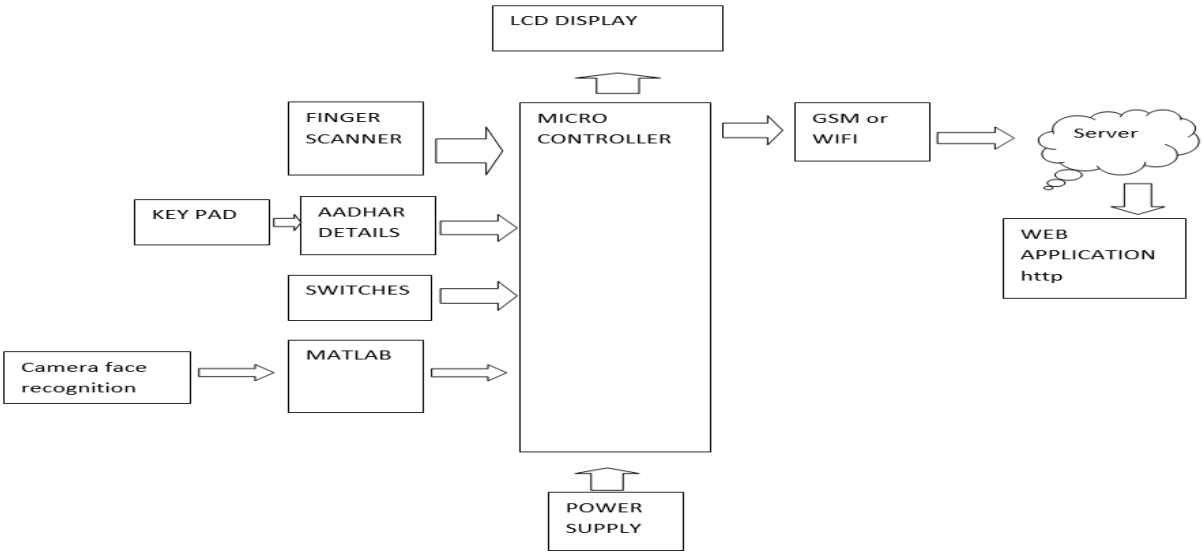


Fig 2.1.1: Sensor interfacing block diagram

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

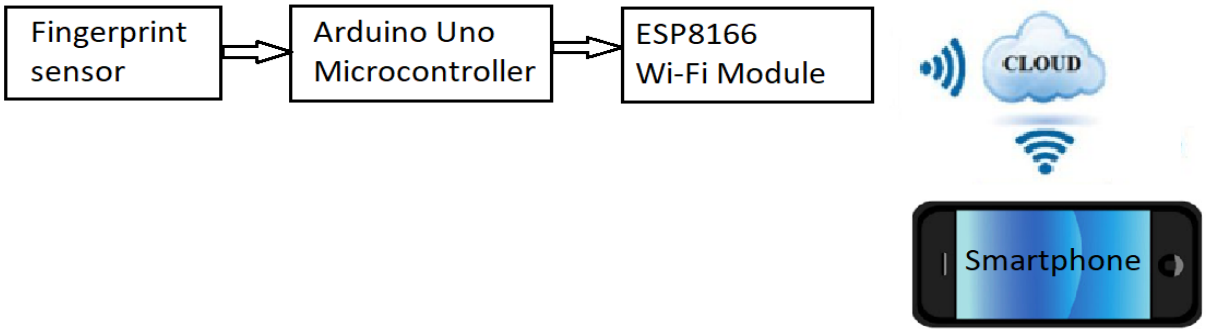


Fig 2.1.2: Block Diagram of the Hardware and Software

III. DESIGN AND IMPLEMENTATION

A. Hardware Implementation

1)ESP8266 Wi-Fi Module

1. It includes a microprocessor which can be programmed directly via the Arduino IDE.

2. To control things there is no need to have the Arduino itself to the interface because the ESP8266 have 39 GPIOs.
3. Operating Temperature Range:- -40c to 125c
4. Operating Voltage Range:- 3.0v – 3.6v

2) R307 Fingerprint sensors

1. Storage Capacity is 1000
2. Operates at 3.3v
3. Fingerprint Comparison (1:1)
4. Fingerprint Search (1: N) function
5. No need of External DSP Chip algorithm

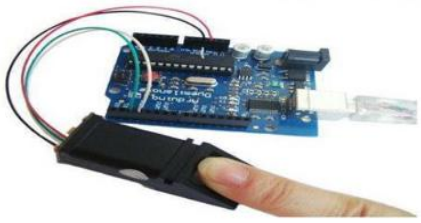


Fig 3.1.2 R307 Fingerprint sensor

3)Arduino mega 2560 microcontroller

1. The **Arduino Mega** 2560 is a **microcontroller** board based on the ATmega2560.
2. It has 54 digital input/output pins (of which 15 can be used as PWM outputs), 16 analog inputs.
3. 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator.
4. A USB connection, a power jack, an ICSP header, and a reset button

4)16×2 LCD module

Voltage is 4.7V to 5.3V and Current consumption is 1mA without backlight. .Alphanumeric LCD display module, meaning can display alphabets and numbers consisting of two rows and each row can print 16 characters.Each character is built by a 5×8 pixel box that can work on both 8-bit and 4-bit mode. It can also display any custom generated characters. Available in Green and Blue Backlight.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

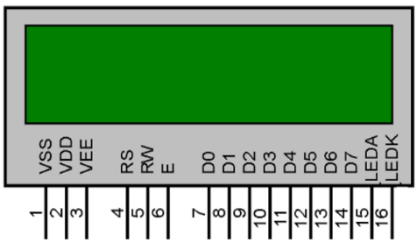


*Fig. 3.1.4: 16*2 LCD Display*

5)Apache server

Available on all platforms – Linux, Windows, MacOS, and other platforms.It's the default server for all C Panel shared hosting, making it effortless to set up and change sites.Tons of functionality offered through a large collection of modules. No matter how obscure your needs be, there's sure to be an existing module for Apache. **As** Per-directory configuration through .htaccess files.Support for HTTP/2, compression, static files, and load balancing.MPM and Fast CGI modes for delivering high concurrency.

B.Software Implementation

1)Architecture and flowchart of online voting system based on Aadhaar

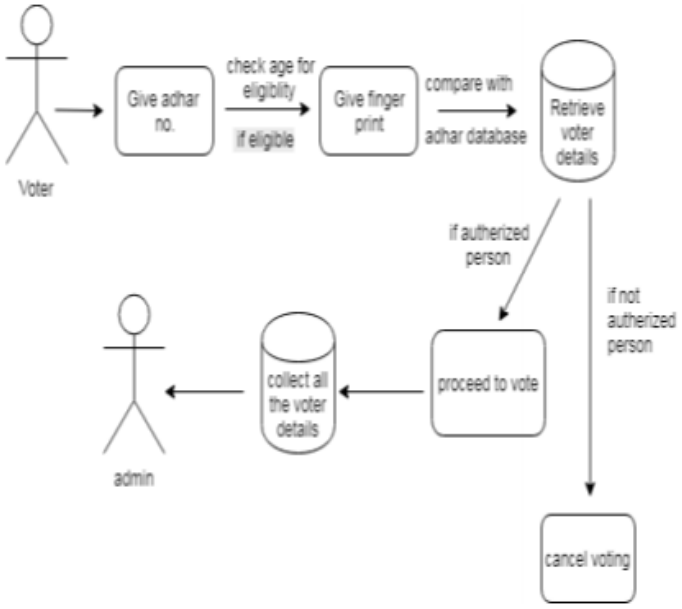


Fig 3.2.1 flowchart of online voting system using aadhaar

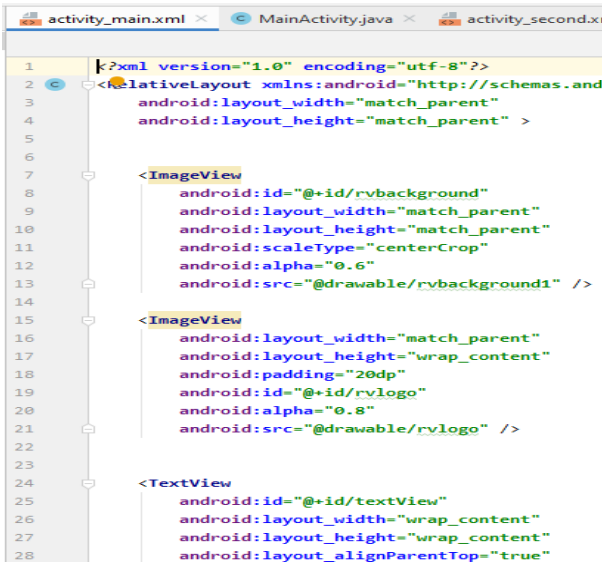


Fig 3.2.2 Java based coding

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

B.XML for front end programming.

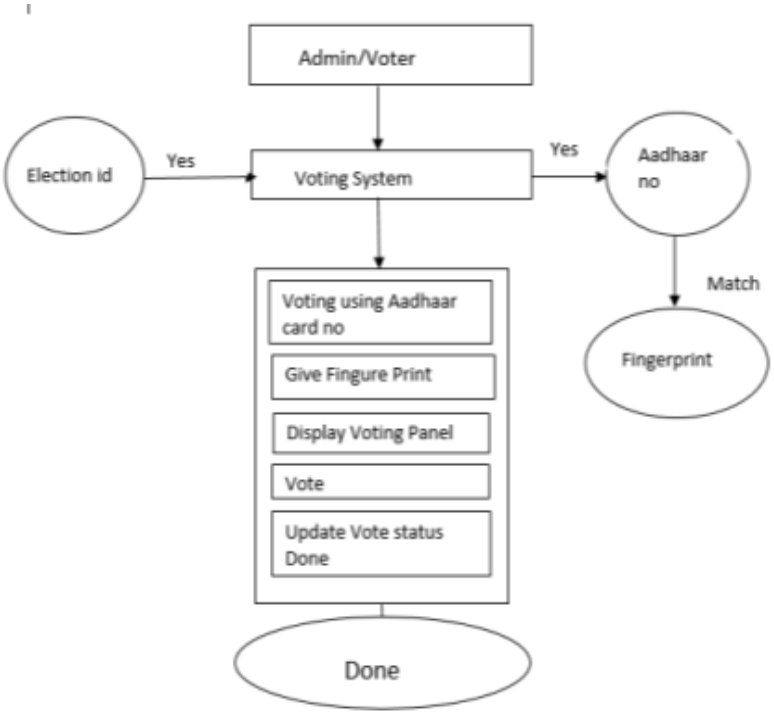


Fig 3.2.3 flow chart with front end panel

C.Software explanation

Web server created can accessed by local networks for our application we need to access by Private Network

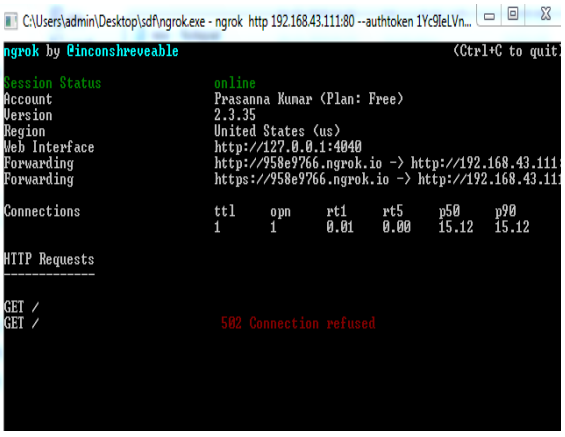
Case 1:

1. Here we created the URLby using port 80 of web server.

2. But port 80 is default port and we cannot use that.

3. Hence we got the “502 connection refused” error

4. Fig 3.2.3 shows the connection refused.



Case 2:

1. Here the URL is tuned successfully

2. But we are getting “ 502 bad gateway

3. Because local host is not properly communicating.

4. Fig 3.2.4 shows failure to complete auto connection

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

IV.CLOUD COMPUTING

A. Vulnerabilities

1. Session Riding**:** Session riding happens when an attacker steals a user's cookie to use the application in the name of the user. An attacker might also use CSRF attacks in order to trick the user into sending authenticated requests to arbitrary web sites to achieve various things.

2. Virtual Machine Escape: In virtualized environments, the physical servers run multiple virtual machines on top of hypervisors. An attacker can exploit a hypervisor remotely by using a vulnerability present in the hypervisor itself – such vulnerabilities are quite rare, but they do exist.

3. Reliability and Availability of Service: We expect our cloud services and applications to always be available when we need them, which is one of the reasons for moving to the cloud. But this isn't always the case, especially in bad weather with a lot of lightning where power outages are common. .

4. Insecure Cryptography: Cryptography algorithms usually require random number generators, which use unpredictable sources of information to generate actual random numbers, which isrequired for full entropy.

Including CSP's should not gain any information of the data. Meanwhile, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and data sharing, without the leakage of the data contents to CSPs or other adversaries.

2. Access controllability

Access controllability means that a data owner can perform the selective restriction of access to their data outsourced to the cloud. Legal users can be authorized by the owner to access the data, while others can not access it without permissions. Further, it is desirable to enforce fine-grained access control to the outsourced data, i.e., different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments

3. Integrity

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that her or his data in a cloud can be stored correctly and trustworthily. It means that the data should not be illegally tampered, improperly modified, deliberately deleted, or maliciously fabricated. If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users.

V. CONCLUSION

By using the concept of cloud computing and secure apache servers we were able to store and retrieve a large amount sensitive information while maintaining maximum security for the voter. As the voter can now vote from his/her own place the voter need not worry about the transparency of the system and can be assured that his/her vote holds equal weightage as any other. The security system of the cloud servers is heavily encrypted ensuring integrity of the system which no hacker can bypass. Hence by combining the concept of hardware and software we are able to achieve a reliable system for security, functioning and storage.

VI. RESULTS

A. Expected Outcomes

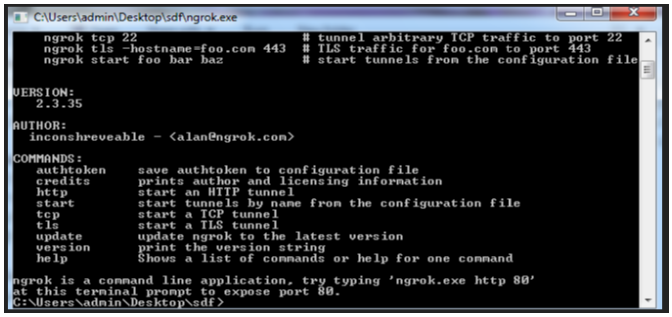
The proposed secured Online voting system uses Aadhaar card and Voter Id for authentication. Database consisting of the details like name, address, age, gender and fingerprint should be updated every time before election. This system affords additional security by allowing voter to vote only once by comparing unique identification. Our main proposal is to enable the user to cast his vote using OVS without going to booth. User can cast his vote from his home or any way and to reduce the proxy vote and in booth capturing situation.

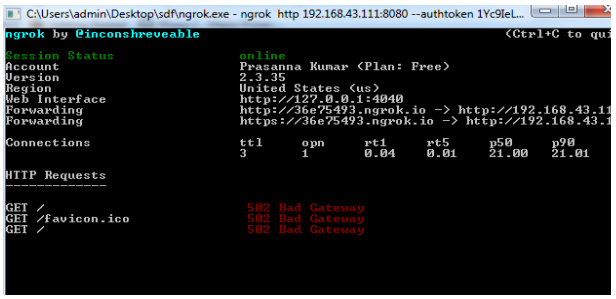
| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

Fig 5.1 Expected login output

B. **Intermediate Results**





REFERENCES

[1] Alaguvel.R1, Gnanavel.G2, Jagadhambal.K3, Biometrics Using Electronic Voting System with Embedded Security, Vol. 2, Issue. 3, March 2019

[2] Mr. S. Glad win Moses Stephen, "AADHAR Based Voting System Using Biometric Authentication and IOT ", March 2017

[3] Prof. R. L. Gayle, Vishnu Lokhande, Shubham T. Jadhav, Aadhaar Based Electronic Voting System" International Journal of Advance Scientific Research and Engineering Trends, May 2016

[4] B. Mary Haque G. M. Owais Ahmed, "Fingerprint and RFID Based Electronic Voting System Linked with Aadhaar For Rigging Free Election", International Journal of Advance Research in Electrical, Electronic and Instrumentation Engineering, March 2016.

[5] Smita B. Khairnar P. Sanyasi Naidu, ReenaKharat, "Secure Authentication for Online Voting System" International Journal of Computer Science and Information 2019.

[6] SoumyajeetChakraborty, AridathaMuncher, Swastika Astrakhan, KassiTaniYasmin "Biometric Voting System using AADHAR Card in India" International Journal of Innovative Research in Computer and Communication Engineering 2019.

[7] Sanjay Kumar Premarket Sing, "Design a Secure Electronic Voting System Using Fingerprint Technique", IJCSI International Journal of Computer Science Issues, Vol.10, Issue 4, 2018.

[8] Alaguvel.R1, Gnanavel.G2, Jagadhambal.K3, Biometrics Using Electronic Voting System with Embedded Security, Vol. 2, Issue 3, March 2013.

[9] Firas I. Hazzaa1, Seifedine Kadry2, OussamaKassem Zein3, Web-Based Voting System Using Fingerprint: Design and Implementation, Vol. 2, Issue.4, Dec 2018.

[10] Malwade Nikita1, Patil Chetan2, Chavan Suruchi3, Prof. Raut S. Y4, Secure Online Voting System Proposed by Biometrics And Steganography, Vol. 3, Issue 5, May 2017.

[11] Ankit Anand1, Pallavi Divya2, An E_cient Online Voting System, Vol.2, Issue.4, July-Aug. 2017, pp2631-2634.

[12] Alaguvel.R1, Gnanavel.G2, Jagadhambal.K3, Biometrics Using Electronic Voting System with Embedded Security, Vol. 2, Issue. 3, March 2019.