AADHAR CARD BASED EFFICIENT BIOMETRIC VOTING SYSTEM

Susan M George[1] ,Nezrin Naushad[2], Nourin Naushad [2], Sneha Anna koshy[2]

Assistant Professor, Department of Computer Engineering, Mar Baselios Christian College of Engineering and Technology, Peermade, Kerala, India[1]

B.Tech Student, Department of Computer Engineering, Mar Baselios Christian College of Engineering and Technology, Peermade, Kerala, India[2]

Abstract: In a democratic country like India an efficient voting system is essential. That's why an Aadhar card based efficient biometric voting system has become necessary. The conventional voting system does not consider any biometrics. This paper attempts to provide a secure and transparent voting system. Biometrics is the term given to the use of biological traits or behavioral characteristics to identify an individual. Biometric Voting System (BVS) which will access the data stored in the database of Aadhar card, a Government Id card for each citizen in India, while casting their votes. Aadhar card consist of our biometric features such as fingerprint image and iris image. For the authentication of a genuine voter the BVS is integrated with a biometric fingerprint machine on the Election Day by comparing the given image with the already stored fingerprint image of that voter in the Aadhar card database. If this system is employed the elections would be fair and free from rigging.

***IndexTerms* - Aadhar, Biometric, Electronic Voting, Fingerprint verification.**

I. INTRODUCTION

Ballot paper system and Electronic voting system are the two types of voting system followed in India. In the Ballot Paper system people need to cast their votes on a piece of paper issued by Election Commission of India. After casting the vote they need to drop that paper in the Ballot Box. The Electronic Voting Machine consists of two units, Control Unit and Ballot Unit. In the Electronic Voting Machine system people need to cast their vote by pressing a button against the candidate and the political party in the Ballot Unit. The vote will automatically be updated against the candidate in the Control Unit of that machine because they are interlinked with a cable. This control Unit is operated by the presiding officer. But both the systems do not provide proper security and authenticity.

In electronic voting system, vendors and election jurisdictions generally state that they do not transmit election results from precincts via the internet, but they may transmit them via a direct modem connection or virtual Private Network(VPN). However, even this approach may be subject to attack via the internet, especially if encryption and verification are not sufficient. This may lead to vulnerability to hacking. Antisocial activists can easily cast false votes by threatening people and creating terror in the locality. They sometime force genuine voters to cast their votes to a specific party by threatening them. As there is lack of security and authenticity in both systems so election procedure is not becoming transparent too much.

Biometric voting system will achieve and attain the highest possible privacy and security while casting the vote by a voter because, the machine uses biometrics. Every single person in the world has unique fingerprint. The BVS unlocks with identifying the voter by his/her fingerprint and when the voting process is over, the machine can automatically count the number of votes that a candidate has acquired. As the system unlocks the voter to cast his/her vote by identifying his/her fingerprint, so there is very less possibility that antisocial activists cast false votes. Here we are also using MD5 algorithm for password encryption if in case the voter faces any difficulty in biometric voting(injured finger, plastered).

II. RELATED WORK

In [1] the use of biometric authentication is confined to a very limited domain in India in terms of providing public services. The authors have worked over proposing different potential implementation sectors for biometric authentication. Implementation of the proposed techniques would not only help automating the authentication procedure and minimizing human intervention, but would also count as a potential initiative for implementing smart and ubiquitous services in India.

In [2] authors compared many biometric identification techniques. On the basis of which we come to conclude that that it all depends upon the user requirements, hardware cost, enrolment time identification time, acceptance ratio. They select one of the techniques according to the security level of the system and its functionalities along with requirements.

In this paper [3] they proposed a mobile e-voting system that prevents coercion using hybrid authentication, safe information transportation using secure socket layers certificate keys, biometric traits and an existing mobile network infrastructure. The two main advantages are integrated security with the use of biometrics also can increase mobility.

In this paper [4] a multilayer secured, internet based voting system using biometric and wavelet based image watermarking The technique presented here can be extended with administrative part required in e-voting system. Our technique is implemented using DWT including multilayer security by using thumb impression and Arnold transform. Kekre's YCgCb colour spaces are used effectively to provide strong security and high robustness in secure e-voting system.

In [5], they present biometric authentication system using multimodality features based technique. To authenticate valid user, two different kinds of features (fingerprint and knuckle) were extracted from a single user. The two features were fused to get a final feature template and back propagation neural network is trained as a classifier.

In [6] they aim at creating a secure voting system using visual cryptography and secure multi-party computation. Visual cryptography is the method of encrypting the visual data for the authentication of the voter. Visual cryptographic scheme is used to create two shares of fingerprint, one stored at the database and other in the voter's ID card. Secure multiparty computation allows multiple parties to participate in a computation which ensures security accuracy and reliability for voting.

III PROPOSED FRAMEWORK

In our proposed system mainly we are using three modules. They are:

1. Admin module
2. Tester module
3. User module

A description of these modules is given below.

Admin module

In this proposed system the officials of Election Commission of India play the role of Admin of the system. To use the system first they need to register themselves with the system. If anybody is registered already, he/she can at once unlock the Admin Dashboard by typing the username and password in the machine. Those persons who have not registered themselves with the system, they need to register them as an Admin by typing their own Aadhar Card no. in the specified space. The system will then search the Aadhar card details from the "Aadhar" Database. Next to verify the authenticity of the Admin the system will seek the fingerprint image from the user. After getting the fingerprint image, the system will compare the fingerprint with the stored one in the "Aadhar" database and if it is matched then it will allow the user to create his/her own username and password for his/her Admin account. This Admin details will be stored in a separate database named as "Admin" Database.

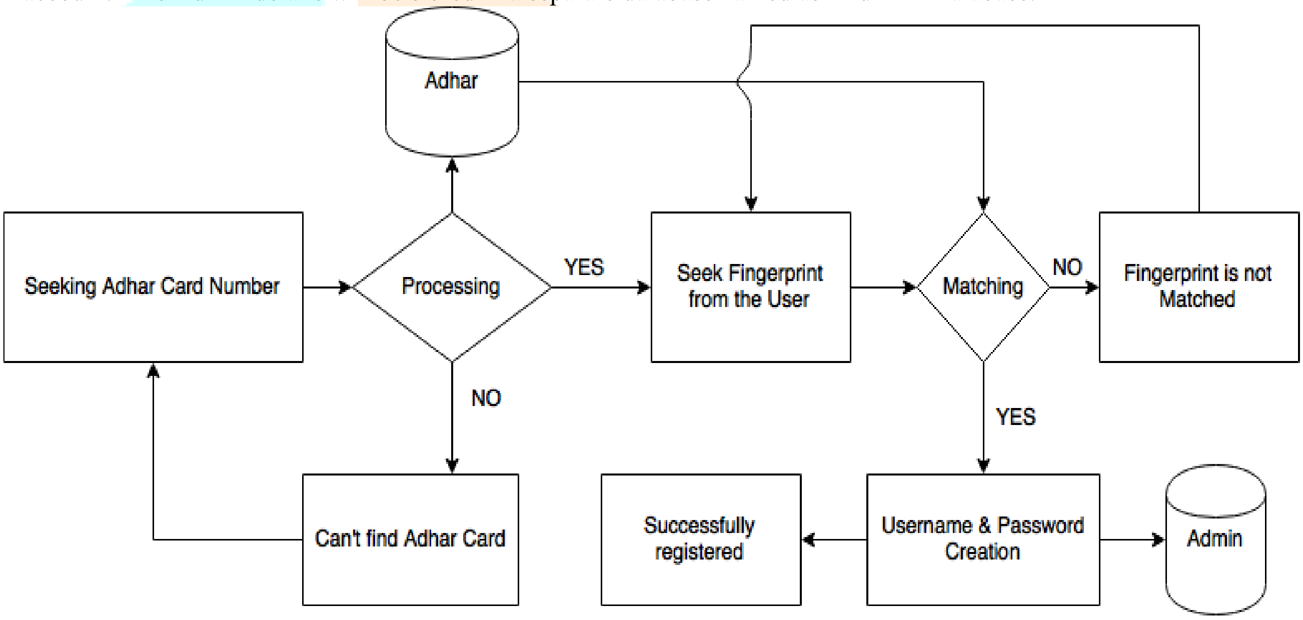
Adhar
Seeking Adhar Card Number
Processing
YES
Seek Fingerprint from the User
Matching
NO
Fingerprint is not Matched
NO
YES
Can't find Adhar Card
Successfully registered
Username & Password Creation
Admin

Fig 3.1: Flowchart of registration process of new admin

The Admin of this system can :

a) **Configure a BVS: -** The admin can configure a BVS for a specific locality for the Election process. It will seek the area first where the election is going to take place. Then it will seek the name of the candidate of a party of that locality and the party symbol. Whenever this information has been given to the system, it will automatically search the Aadhar database with respect to the area and find out the entire person living in that locality.

b) **View the result: -** The system gives a facility to the admin to view the result of the election of a specific locality. It will fetch the vote result from the "Vote Result" database and show it to the admin

c) **See the number of people did not cast vote: -** The admin can see the name of the people of a locality who have not casted their votes. The system can lock the people who have casted their votes properly by changing the lock property to 1 from 0. So, those persons who have not casted their votes, their lock status will remain as 0. The system searches for these person and show the name and Aadhar card details to the admin. Fig 3.2 describes the process how the BVS can find those people who have not casted their votes.

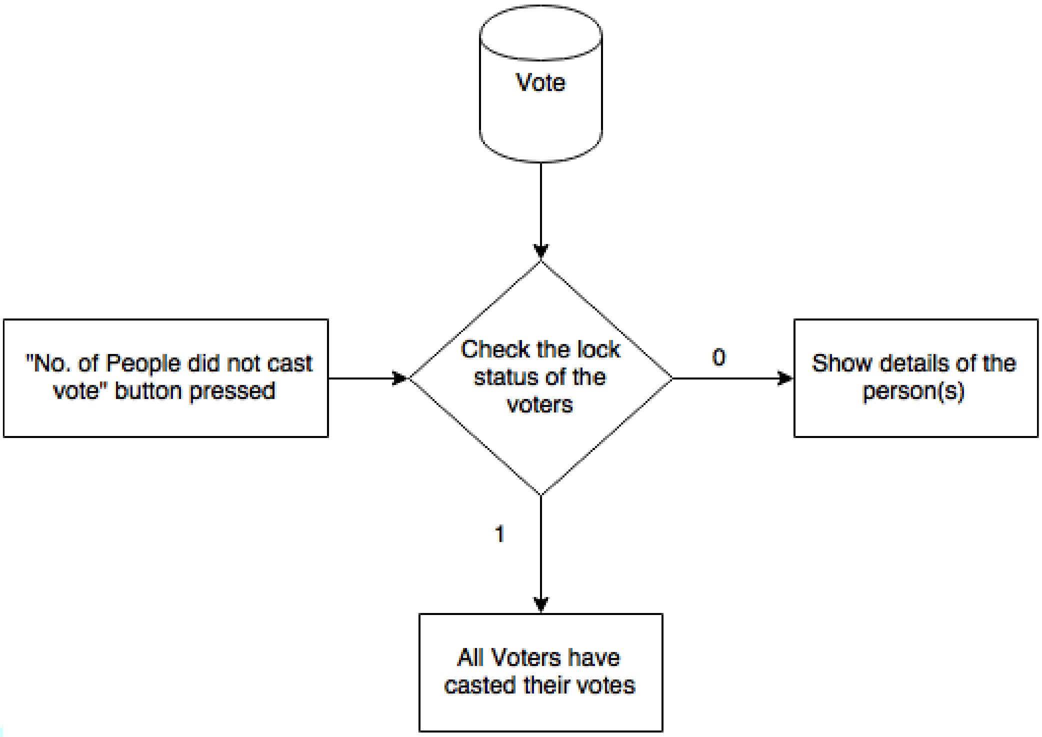
Vote
"No. of People did not cast vote" button pressed
Check the lock status of the voters
0
Show details of the person(s)
1
All Voters have casted their votes

Fig 3.2: Flowchart for not casted votes

d) **Delete vote related data: -** The BVS will also provide delete facility of the previous vote related data in that particular system to the admin. If the admin press the "Delete" button in his/her dashboard then, the system will automatically delete the previous election data in the "Vote" and "Vote Result" databases in that system. This is needed to clean up the databases and to make the BVS ready for the next election. Fig 3.3 describes how the admin can delete the previous election data in a specific BVS.

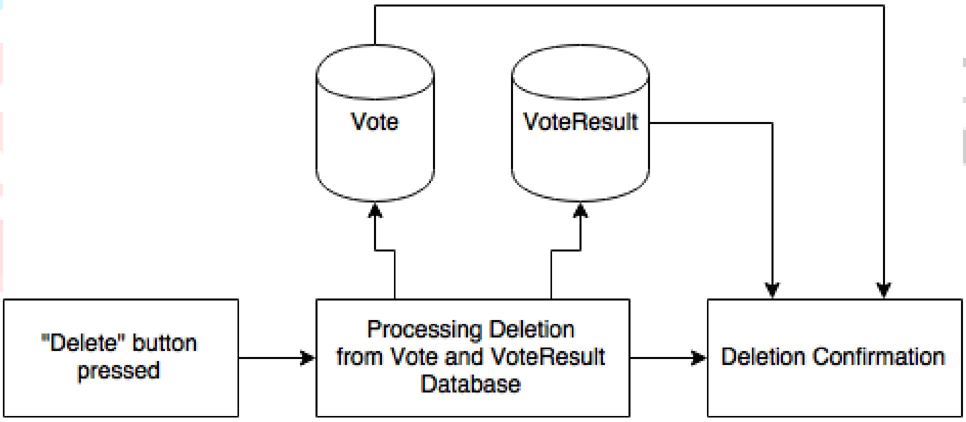

Fig 3.3: Flowchart for admin deletion

e) **Insert people data: -** In every year, huge amount of people are issuing Aadhar card. To include their details in the Aadhar database the BVS provides another facility to the admin. By using a BVS, the officers of the election commission can insert the details of the new Aadhar card issuers directly into the "Aadhar" database. This facility can be used as an immediate measure, just sometime before the election takes place.

TESTER MODULE

This mode is for the presiding officer in the booth. Here he/she can conduct the vote procedure on the Election Day as well as he/she can test the system to check whether it is working perfectly or not, before the Election Day. A presiding officer also needs to open an account in the BVS. Otherwise he/she cannot operate the system. Those who are already registered as a Tester they can login with their username and password and can see the various options on their dashboard. Those who are not registered, they need to register themselves first with the BVS. The registration process is identical to the new admin registration process. The only difference over here is that the data of the Tester will save in a separate database called "Tester" rather than "Admin" database.

The presiding officer can –

a) **Give Test Votes: -** This is identical to User Mode. It is described later. To test the BVS whether it is actually working perfectly or not, whether it is counting the number of votes a candidate is gaining perfectly or not, the presiding officer choose this option on his/her dashboard. He/she can give test votes and later he/she can delete these votes also before the Election Day.

b) **View Result: -** The presiding officer can see the result of the election of a particular locality by pressing the "View Result" button. The process to view the result is identical to the "View Result" option of admin which is already discussed earlier.

c) **See the number of people did not cast vote: -** By utilizing this facility the presiding officer can see the name and Aadhar card number of the persons who did not cast their votes. This procedure is also identical to the "see the number of people did not cast vote" procedure of the admin which is discussed earlier.

d) **Delete test votes: -** After casting test votes the presiding officer has to delete the vote data. Otherwise, it will be counted with actual vote. Whenever the "Delete" button is clicked, the system will search for the update made on "Vote" and "Vote Result" database. When the update is found, the updated data is taken back to its default state by the BVS.

e) **Unlock intentionally locked persons: -** One of the most important feature of the BVS is to unlock the intentionally locked persons by the presiding officer. While comparing the fingerprint of a voter if the BVS find that there is no matching in between the given fingerprint and the stored fingerprint of that voter in his/her Aadhar database then it will automatically lock the person thinking him/her as a fraudulent voter. To unlock this lock the presiding officer will check the documents of the voter. If he/she is proved authenticated then the presiding officer will press the Unlock intentionally lock" button and the BVS will change the lock state of that person from 1 to 0 and let him/her to give another chance to cast his/her vote.

f)**Activate User Mode: -** This is the most important option of the Tester Mode. By default the User Mode is disabled due to the testing purpose of the machine. But if the presiding officer activates the User Mode then it will run in an infinite loop to get the votes of the general voters. Along with that if the User Mode has been activated then the Delete feature of the Tester Mode will be deactivated. Because by somehow if the delete button has been pressed by anyone unknowingly or knowingly then all the vote related data will be deleted. To get out of the infinite loop the presiding officer needs to hit the "Set User Mode Off" button.

USER MODULE

This mode is for the general voters. At first they need to enter the Aadhar card in the BVS. The BVS will search that Aadhar Card number in the "Vote" database in place of "Aadhar" database because while configuring the machine the BVS had already selected the Aadhar details of the people of a specific locality from the Aadhar database and stored it into the "Vote" database. Next it will seek the fingerprint image from the voter with which it will compare the stored image in the "Vote" database. If the matching is successful then the BVS will take the voter to the Vote page where the voter will get the selection option for his/her liked candidate. If the fingerprint is not matched perfectly then it may seek the fingerprint image again from the voter [5]. But if the BVS find the given fingerprint image by the voter is completely different from the stored fingerprint in the database then the system will automatically lock that voter thinking him/her as a fraud. The unlocking process is mentioned previously.

If the voter comes to the Vote giving page, then he/she can choose anyone among the candidate whom he/she likes mostly. Thereafter the BVS will automatically lock that Aadhar card number by changing the lock property from 0 to 1. Simultaneously at the same time it will update the "vote Result" database by increasing the "no. of vote" attribute of the selected candidate by one. After successfully update these two databases the BVS will show the voter the confirmation.

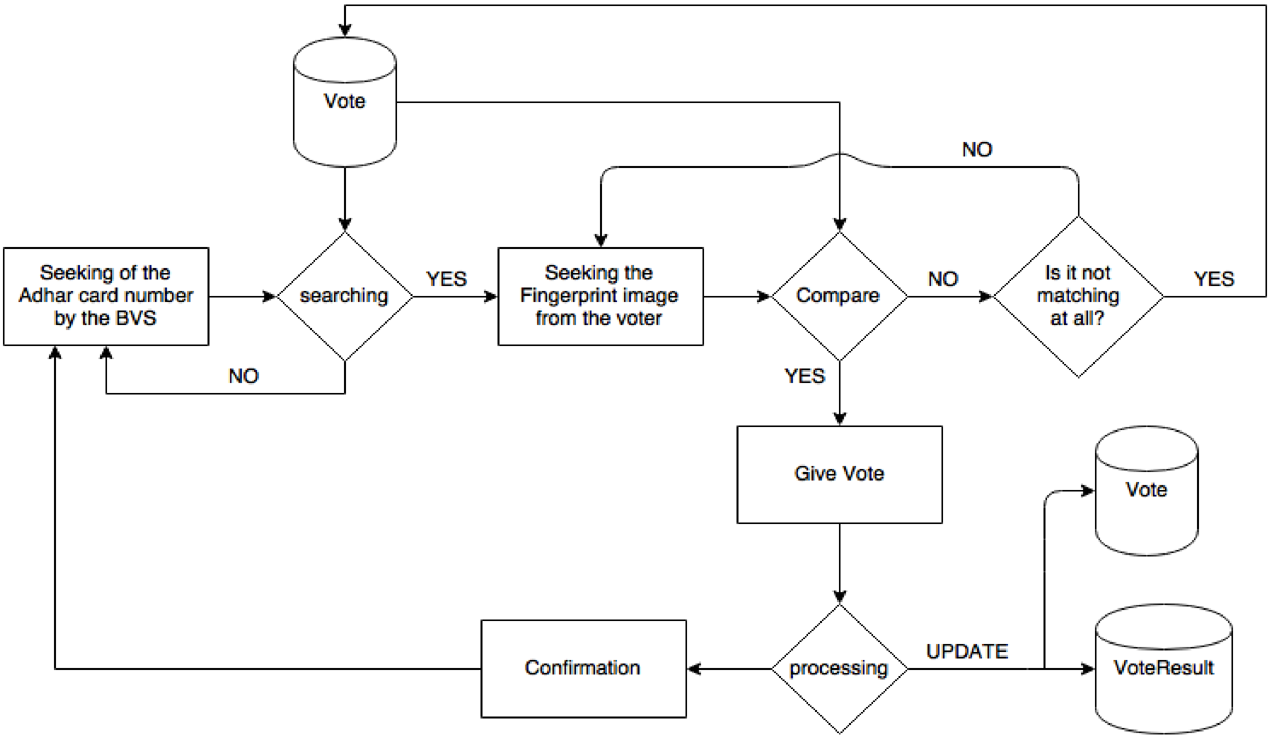
Vote
NO
Seeking of the Adhar card number by the BVS
searching
YES
Seeking the Fingerprint image from the voter
Compare
NO
Is it not matching at all?
YES
NO
YES
Give Vote
Vote
Confirmation
processing
UPDATE
VoteResult

Fig 3.4: Flowchart for user

MD5 Algorithm

The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. Like most hash functions, MD5 is neither encryption nor encoding. It can be cracked by brute-force attack and suffers from extensive vulnerabilities

Step 1. Append Padding Bits

The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. That is, the message is extended so that it is just 64 bits shy of being a multiple of 512 bits long. Padding is always performed, even if the length of the message is already congruent to 448, modulo 512.

Step 2. Append Length

A 64-bit representation of b (the length of the message before the padding bits were added) is appended to the result of the previous step. In the unlikely event that b is greater than 2^64, then only the low-order 64 bits of b are used. (These bits are appended as two 32-bit words and appended low-order word first in accordance with the previous conventions.)

Step 3. Initialize MD Buffer

A four-word buffer (A, B, C, and D) is used to compute the message digest. Here each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first

Step 4. Process Message in 16-Word Blocks

We first define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

Step 5. Output

The message digest produced as output is A, B, C, and D. That is, we begin with the low-order byte of A, and end with the high-order byte of D.

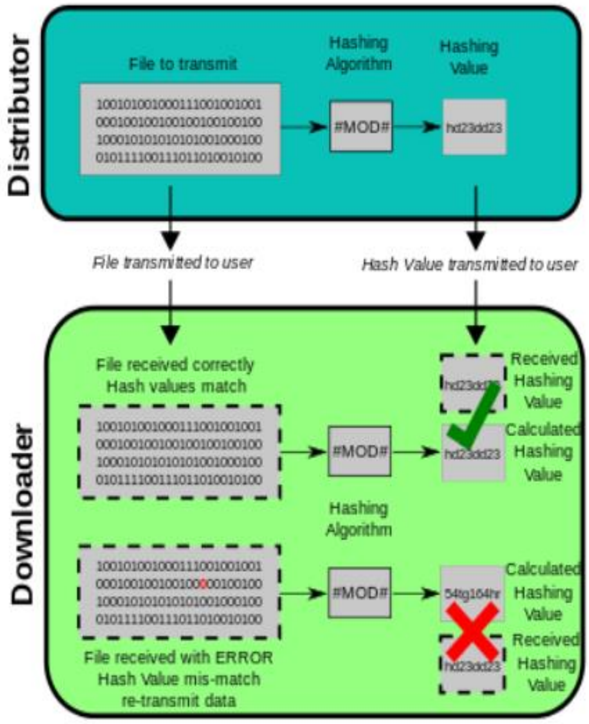

Fig 3.5: Application of MD5 algorithm

IV.HARDWARE MODULES

There are two hardware modules

1. Fingerprint Module
2. Wi-Fi Module

Fingerprint Module

The fingerprint scanner itself does all of the heavy lifting behind reading and identifying the fingerprints with an on-board optical sensor and 32-bit CPU. It can store up to 200 fingerprints in its inbuilt memory. Each fingerprint that you want to store should be registered by sending the corresponding command and pressing your finger against the reader three times. The fingerprint scanner can store different fingerprints and the database of prints can even be downloaded from the unit and distributed to other modules.

Wi-Fi Module

The Wi-Fi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your Wi-Fi network. It is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor. Each ESP8266 module comes pre-programmed with an AT command set firmware, meaning, you can simply hook this up to your Arduino device and get about as much Wi-Fi ability as a Wi-Fi Shield offers.

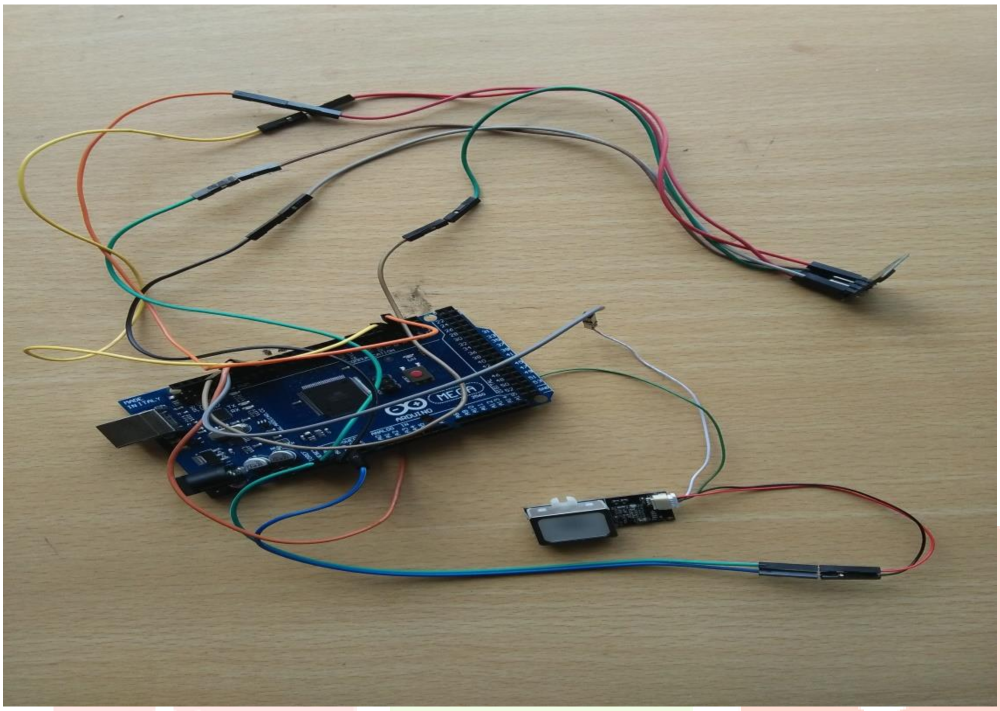

Fig 4.1: Hardware Portion

V. Conclusion and Future Work

Throughout this paper a maiden overview of a Biometric Voting System is presented which can be implemented in the elections of India to prevent the antisocial activities in the booth [1]. This system can be implemented in other countries also where the government of that country issues card like Aadhar card for the citizen. It is too much fast to do the tasks and most of the tasks are done automatically by the system so that, there will be no problem of manual discrepancies. The cost of the system will not be so high. Biometric devices are highly used in most of the organizations now-a-days. So it is not too much strenuous task for any organizations like Election Commission of India to bear the expense of this system. The system is too much accurate about the Vote Result and it is fast too for doing the tasks. Elections results can be declared very soon by utilizing this system and we will get an actual transparent election [1].

1). Iris scan also be included to make the security of this system much higher. Iris image is already there in the Aadhar card database of every citizen of India. So it can be implemented without facing any difficulties [2], [4].

2). this system can be put into a small special room where only one person can enter. In that room there may be heat sink or laser by which the system can understand the presence of only one person in the room. If somehow there are two persons in the room then the system will block itself and prevent both of those persons to cast vote.

3). we have used the correlation-based fingerprint matching technique in our system. To improve the performance and to get a much reliable fingerprint recognition and authentication system the other two algorithms can be used.

References

[1] Biometric Authentication for UID-based Smart and Ubiquitous Services in India
[2] A Comprehensive Study of Various Biometric Identification Techniques
[3] Secure e-voting system with biometric and wavelet based watermarking technique in ycgcb colour space
[4] Biometric Identification System using Fingerprint and Knuckle as Multimodality Features
[5] Privacy-Preserving Biometric Identification Using Secure Multiparty Computation

[6] E-Voting System Using Visual Cryptography & Secure Multi-party Computation