Biometric Voting System using Adhar Card in India

Soumyajit Chakraborty[1], Siddhartha Mukherjee[1], Bhaswati Sadhukhan[1], Kazi Tanvi Yasmin[1]

B.Tech Student, Dept. of CSE, Narula Institute of Technology, Agarpara, Kolkata, India[1]

ABSTRACT: The paper will give an overview of a Biometric Voting System (BVS) which will access the data stored in the database of Adhar card, a Government Id card for each citizen in India, while casting their votes. While issuing the Adhar card a citizen of India needs to give his/her unique biometric data i.e. the fingerprint image and iris image of both eyes to the government. The BVS is integrated with a biometric fingerprint machine for the authentication of a genuine voter on the Election Day by comparing the given image with the already stored fingerprint image of that voter in the Adhar card database. This system has been developed in Microsoft Visual Studio 2015 with the help of ASP.NET, c# and SQL Server 2014 [1]. To eradicate the evil of vote rigging now-a-days in several elections in India, this proposed system can be implemented to get a transparent election in future [2].

KEYWORDS: Adhar, Biometric, Electronic Voting, Fingerprint verification, Offline voting

I.   INTRODUCTION

In India there are two types of voting procedure which are used to be followed during an election. The first one is Ballot Paper System and the second one is Electronic Voting System (EVM).

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 cannot achieve and attain proper security and authenticity. 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.

To get rid of this serious problem, Biometric voting system can be used for any election procedure. It 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. So, we can achieve a transparent vote [1], [2].

II.   BIOMETRIC METHOD

The main focus of the proposed system is the use of fingerprint image of a voter to authenticate him and to cast the vote very securely. Fingerprint matching techniques can be classified into three types –
 • **Correlation-based matching [6]:** Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).
 • **Minutiae-based matching [6]:** This is the most popular and widely used technique. Minutiae are extracted from the two fingerprints and stored as sets of points in the two- dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

• **Pattern-based (or image-based) matching [6]:** Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

A fingerprint recognition system operates either in verification mode or in identification mode. The various stages in a fingerprint verification system are shown in Fig 0.1 [3].
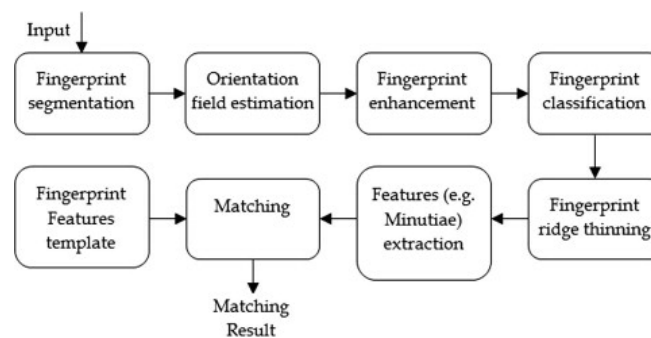

Fig 0.1: Architecture of Fingerprint Verification

In the proposed Biometric Voting System (BVS) we have used the correlation-based matching procedure to identify person from his/her fingerprint.

III. PROPOSED FRAMEWORK

Our proposed system mainly works in offline mode and has three modes. They are –
1. **Admin Mode**
2. **Tester Mode**
3. **User Mode**

Here is the brief description of these three modes.

1. ADMIN MODE

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 Adhar Card no. in the specified space. The system will then search the Adhar card details from the "Adhar" 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 "Adhar" 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. Fig 1.0 in the next page demonstrates the process.
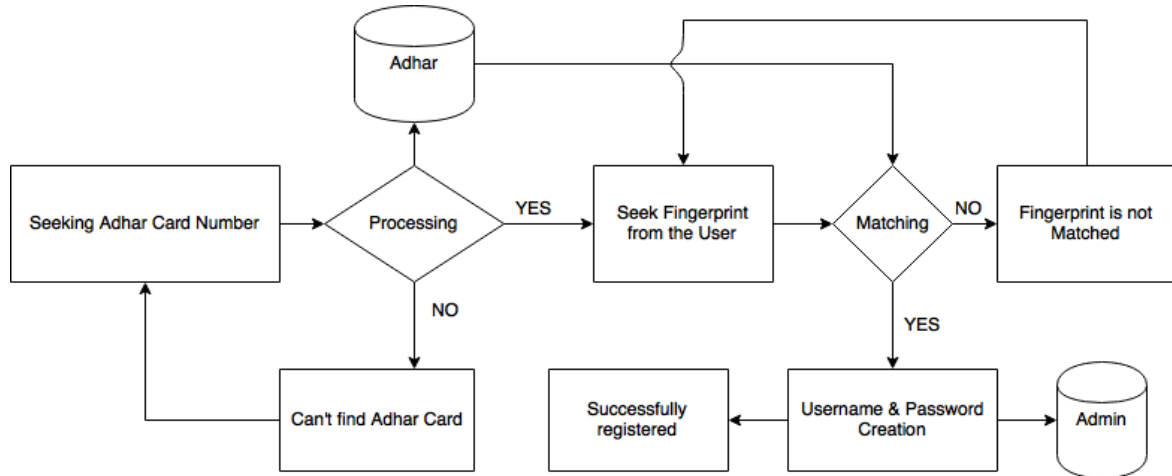
Fig 1.0: Flow Chart of registration process of a new Admin in the BVS

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 these information has been given to the system, it will automatically search the Adhar database with respect to the area and find out all the person living in that locality. Then it will store those
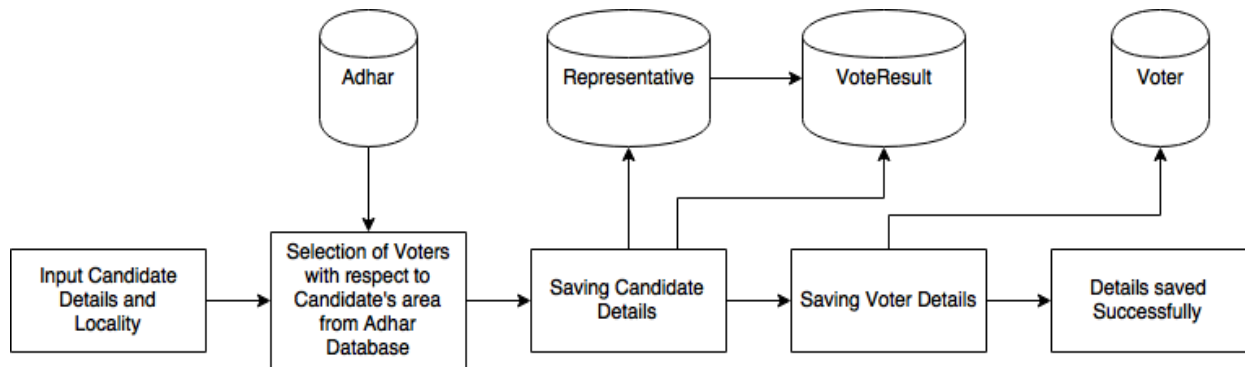

Fig 1.1: Flow Chart of Configuration of the BVS

persons' details in "Vote" database. Simultaneously it will also store the candidate details in "Representative" database. The BVS will select some attributes like name, candidate_id, party emblem and No_of_votes_gained attribute in "VoteResult" database. This database will be used to update the number of votes gained by a candidate while voting process. So, by pressing one button the system will automatically configure itself for a specific locality. No manual effort is needed for searching and making a list of the voters in that locality. Fig 1.1 demonstrates the process of configuring the BVS.

   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 "VoteResult" database and show it to the admin. Here the admin can see the result
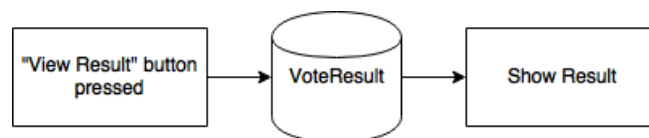

Fig 1.2: Flow Chart for View Election Result

of all the candidates of a specific locality. Fig 1.2 demonstrates the process for viewing result.

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 Adhar card details to the admin. Fig 1.3 describes the process how the BVS can find those people who have not casted their votes.
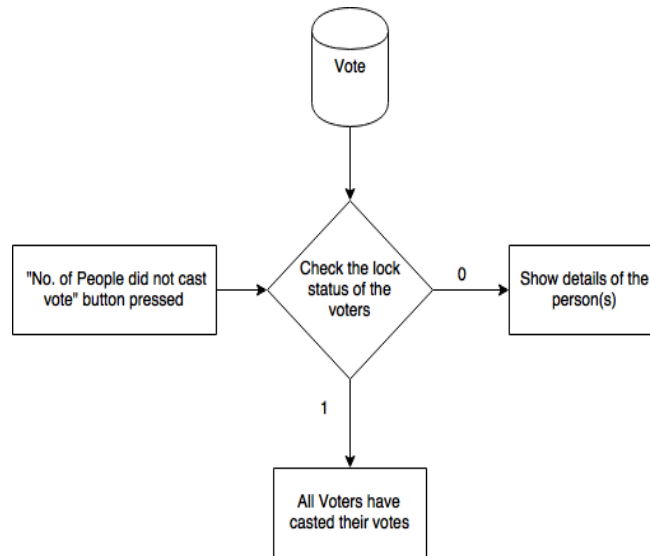

Fig 1.3: Flow Chart to see how many people have not casted there votes

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 "VoteResult" databases in that system. This is needed to clean up the databases and to make the BVS ready for the next election. Fig 1.4 describes how the admin can delete the previous election data in a specific BVS.
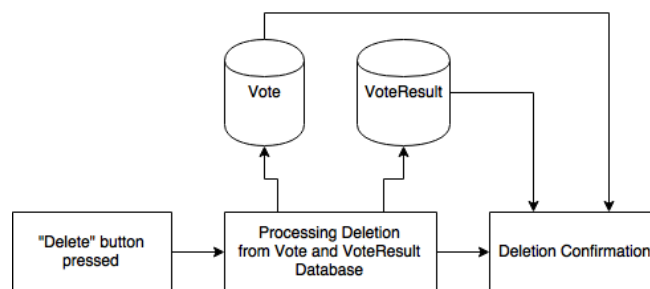

Fig 1.4: Flow Chart for Admin Deletion

International Journal of Innovative Research in Computer and Communication Engineering

e). Insert people data: - In every year, huge amount of people are issuing Adhar card. To include their details in the Adhar 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 Adhar card issuers directly into the "Adhar" database. This facility can be used as an immediate measure, just sometime before the election takes place. The system will seek all the personal
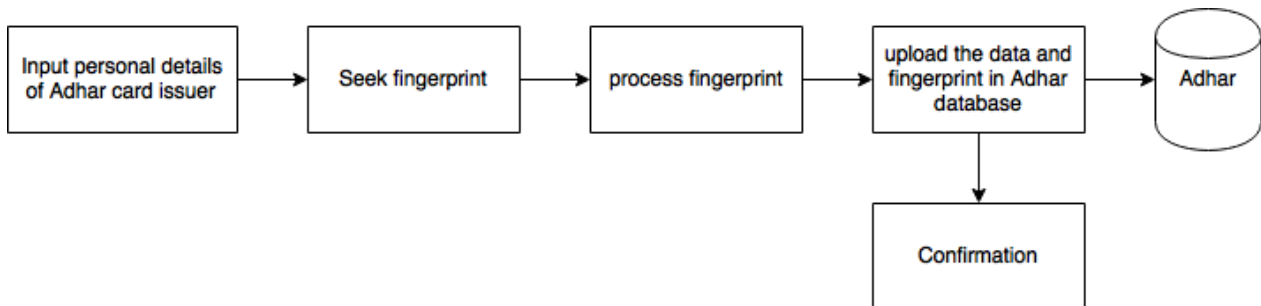

Fig 1.5: Flow Chart for Inserting Adhar details in Adhar database

details and fingerprint image of the Adhar card issuer. Then it will process the data and store it into the "Adhar" database. Fig 1.5 shows how an admin can insert Adhar details of a person into "Adhar" database.

II. TESTER MODE

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 need 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 Adhar 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 "VoteResult" database. When the update is found, the updated data is taken back to its default state by the BVS. Fig 2.0 in the next page shows how a presiding officer can delete the test votes given by him/her.
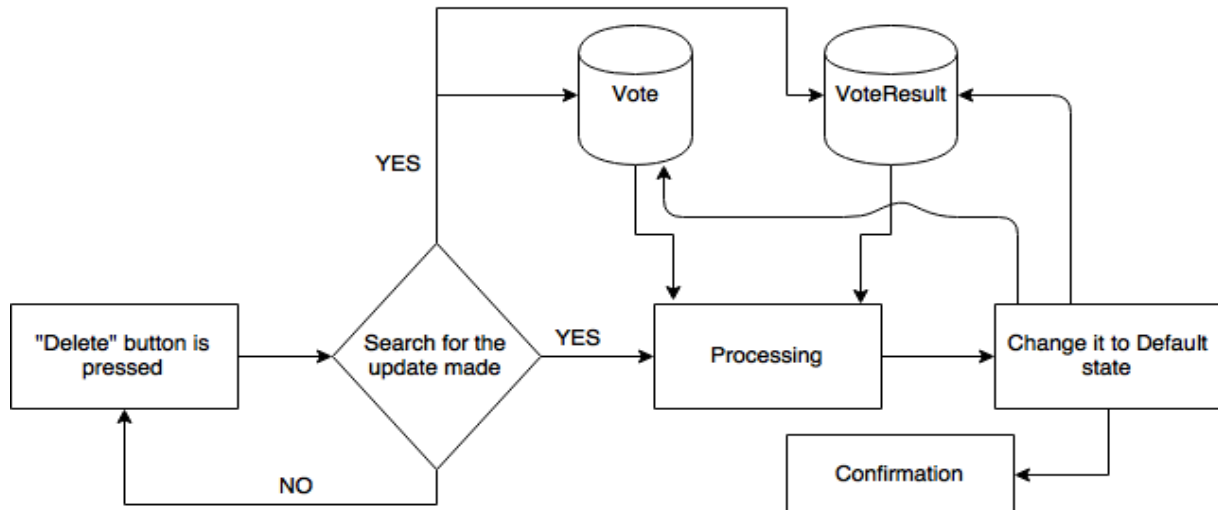
Fig 2.0: Flow Chart for deletion by the Tester

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 Adhar 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
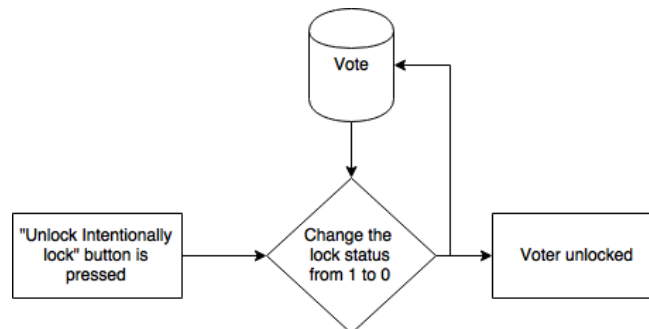

Fig 2.1: Flow Chart for unlocking an intentionally locked

"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. The process for unlocking an intentionally locked person has been described in Fig 2.1.

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.

III. USER MODE

This mode is for the general voters. At first they need to enter the Adhar card in the BVS. The BVS will search that Adhar Card number in the "Vote" database in place of "Adhar" database because while configuring the machine the BVS had already selected the Adhar details of the people of a specific locality from the Adhar 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], [8]. 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 Adhar card number by changing the lock property from 0 to 1. Simultaneously at the same time it will update the "VoteResult" 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
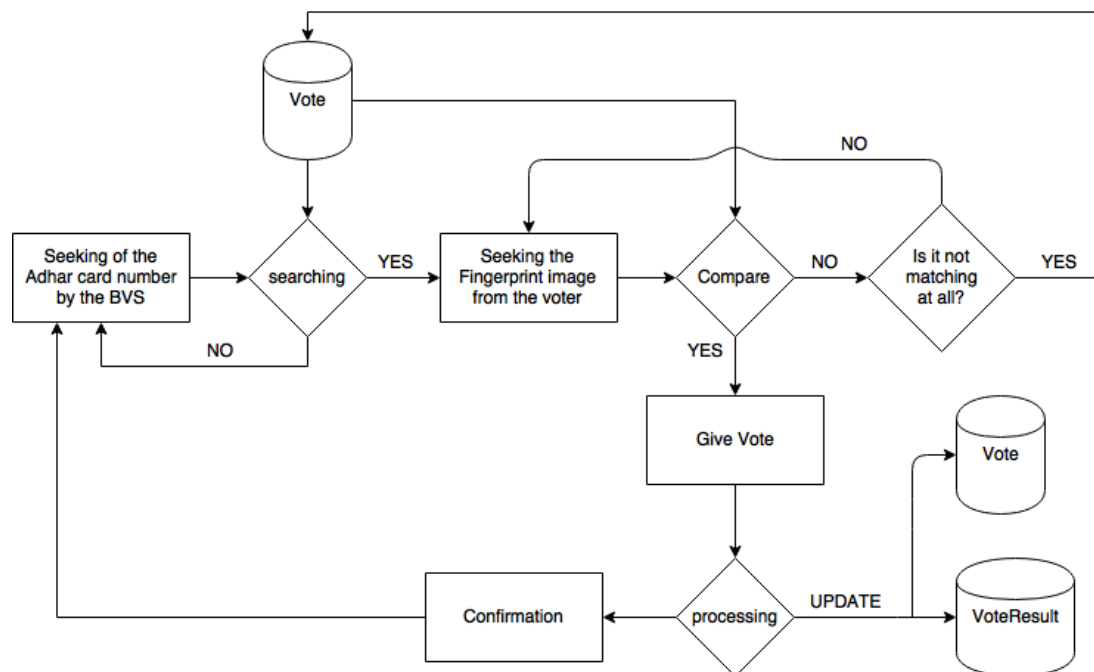

Fig 3.0: Flow Chart for User Mode

message about his/her successful vote. Fig 3.0 describes how a general voter can cast his/her vote in the BVS and after successful vote he/she gets the confirmation message that his/her vote has been successfully processed.

IV. CONCLUSION

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 Adhar 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 [7]. 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].

V. FUTURE WORKS

1). Iris scan also be included to make the security of this system much higher. Iris image is already there in the Adhar 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.

ACKNOWLEDGEMENT

REFERENCES

[1] M.O Yinyeh and K.A. Gbolagade, Overview of Biometric Electronic Voting System in Ghana, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, page 624-627

[2] Mayuri U. Chavan, Priyanka V. Chavan and Supriya S. Bankar, Online Voting System Powred by Biometric Security using Cryptography and Steganography, International Journal of Advanced Research in Computer Science and Management Studies, volume 1, page 226-231

[3] Ayman Mohammad Bahaa-Eldin, A medium resolution fingerprint matching system, Ain Shams Engineering Journal, Volume 4, pages 393-408

[4] ALaguvel.R, Gnanavel.G and Jagadhambal.K, Biometrics using Electronic Voting System with Embedded Security, International Journal of Advanced Research in Computer Engineering and Technology, Volume 2, page 1065-1072

[5] AdemAlpaslan ALTUN and MetinBiLGiN, Web based secure e-voting system with fingerprint authentication, Scientific Research and Essays, Volume 6(12), page 2494-2500

[6] SangramBana and Dr. Davinder Kaur, Fingerprint Recognition using Image segmentation, International Journal of Advanced Engineering sciences and technologies, Volume 5, page 012-023

[7] Sonja Hof, E-Voting and Biometric Systems? http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-7.pdf, page 63-72

[8] Rohan Patel, VaibhavGhorpade, Vinay Jain and   MansiKambli, Fingerprint Based e-Voting System using Adhar Database, International Journal for Research in Emerging Science and Technology, Volume 2, page 87 - 90

BIOGRAPHY

Soumyajit Chakraborty is a B.Tech student in the Computer Science and Engineering Department, Narula Institute of Technology, Agarpara, Kolkata, India (WBUT).

Siddhartha Mukherjee is a B.Tech student in the Computer Science and Engineering Department, Narula Institute of Technology, Agarpara, Kolkata, India (WBUT). Also received the Diploma in Computer Science and Technology from Nibedita Institute of Technology (WBSCTE) in 2013.

Bhaswati Sadhukhan is a B.Tech student in the Computer Science and Engineering Department, Narula Institute of Technology, Agarpara, Kolkata, India (WBUT).

Kazi Tanvi Yasmin is a B.Tech student in the Computer Science and Engineering Department, Narula Institute of Technology, Agarpara, Kolkata, India (WBUT).