



Novel E-Voting System with Biometric Authentication and Distributed Server System

PP Shendage*, PC Bhaskar

Department of Technology, Shivaji University, Kolhapur, Maharashtra, India

E-mail: shendagepriyanka1@gmail.com

Abstract: India is the largest democratic country where voting and elections are fundamental to any consensus-based society. In India we use the most popular voting system called as an electronic voting system (EVM) for its easy access and less time consuming features, but yet this voting system is not at all efficient and secured one. So we present a Novel Electronic Voting System which is based on biometric authentication and distributed servers approach which provide high security for voting process. Whole voting system is divided into two parts one is a voting machine and another is server system. Raspberry pi 3 model B is a heart of the voting machine. This host minicomputer has the ability to control complete activity of voting process. Voting machine is developed based on biometric authentication and distributed server system. So for authentication purpose we use a biometric database of Aadhar card which is already given from all Indian citizens by the Unique Identification Authority of India (UIDAI). So the voter authentication can be done by using biometric information (Thumb impression) which is pre-stored at the government database. The significance of adding thumb impression results in exact authentication of voter before casting of vote. So the system absolutely adds accuracy of casting of votes and nullifies the chances of malpractices in regard to the casting. The main advantage of this system is, it is based on a distributed server approach, which will ultimately add the accuracy of casting of votes and reduce long distance travelling to cast a vote. Therefore establish a reliable, flexible system which will be easy to handle by all populations considering their literacy and age factor, also to control fake voting which ultimately adds transparency in voting system.

Keywords: Automatic voting machines; Biometric fingerprint authentication; Distributed server; Unique identification authority of India number

I. INTRODUCTION

Elections enable every adult citizen of the country to participate in the process of government formation. You must have observed that elections are held in our country frequently. These include elections to elect members of the Lok Sabha, Rajya Sabha, State Legislative Assemblies (Vidhan Sabhas) Legislative Councils (Vidhan Parishad) and President and Vice-President of India. Elections are also held for local bodies such as municipalities, municipal corporations and Panchayati Raj justifications [1].

Elections are being held in India for selecting the most appropriate and desirable candidate to lead our nation by all citizens of India whose are eligible to cast their vote. So corruption free voting system is important issue at present to select proper candidate for every positions. Now a day manual voting and electronic voting system is used for elections but there is a maximum chance of corruptions, because unfortunately not all e-voting projects succeed in delivering on such high promises. Because in that number of problems are occur such as, a voter could not check what happened to his/her vote i.e., whether it has been properly recorded in the system database or not and also valid voters are just checked by polling officers by their photos on the voter card therefore more or less similar looking persons can give the vote on behalf of another [2-5].

However the present voting system deals with no. of problems such as fake voting and fraud. Due to this the undesirable and worst case candidates gets elected and does not contribute to the development of specific region to which they belong which results in betrayal of society [6]. In addition to this these leaders take full advantage of their power and position to get elected by any means, either by malpractices or by violating the rules and regulations of election commission of India [7].

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

These types of corruptions can be stopped by using our proposed voting system. In This system voters are identity by using biometric authentication process, so it absolutely adds the accuracy of casting of votes and nullify the chances of malpractices in regard to the casting. Also distributed server approach is present in that system means it is connected to the main server in each constituency. So, the vote can be cast irrespective of location of voter where the authentication can be done at any location with the network [8-10].

II. PROPOSED SYSTEM

2.1 Details of Proposed System

Overview:

We can say that this whole voting system is divided into three main parts like BTS, BSC and MSC in GSM architecture. Here BTS means ‘voting processing set up’ which is present in selective locations in all constituencies [11]. This system is based on client server architecture so here BSC means all ‘client/slave servers’ which is implemented on boundary of each constituency and all this client servers are connected to one ‘centralized master server’ which is called as MSC [12].



Figure 1: Architecture of proposed system like GSM architecture.

As in the system, the AVM counters (voting processing setup) will be look like a simple work stations or terminals. In diagram shows a number of distributed servers (database servers), each assembly (situated in the district town) required one database server and should be connected to all terminals throughout the villages/towns [13] as per the population of the concerned constituency or assembly AVM counters can be constructed. And all database servers of each assembly are connected to the one master database server (which is present in one district) [14]. So the whole process is centralized which is show in Figure 1.



Figure 2: Set up of proposed system.

As the process will be completely centralized so, voter of one constituency may cast his/her vote from another constituency because on using the Aadhar card on any AVM the system will show the candidate list for the concerned constituency to which the voter actually belongs. Therefore, after voting the system will automatically store the information to the appropriate block in the system database server [15].

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

Voting processing set up:

Raspberry pi 3 model B is a heart of the voting processing set up. Figure below shows the different peripherals like fingerprint module, keypad, monitor and Ethernet connection are connected to raspberry pi [16-18].

Client/slave server:

All voting set ups which are present in one constituency are connected to one client server which is placed at the boundary of that respective constituency. Biometric database (Aadhaar card data) of each and every voters of that respective constituency is available or store in this server.

Master server:

It is act like a MSC station in GSM architecture. The biometric database (Aadhaar card) of all voters which are present in any constituency is available in master server. So at the time of change in constituency the voter's data is accessed from master server Figure 2.

2.2 Concept of Proposed System using Flow Chart

The proposed system implemented at polling booths where the voter go into voting counter and enter the 12 digit Aadhaar card number by using keys. So by detecting this number the system access the fingerprint of respective voter from UIDAI database. This process is shown in Figure 3.

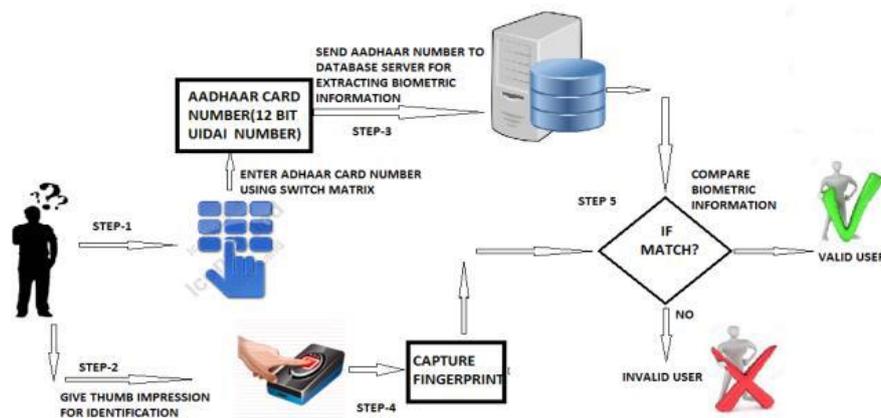


Figure 3: Concept existing of system.

If the fingerprint is match with database information (fingerprint) then the voter is valid else the voter is invalid. Valid voter allow proceeding to voting process and select any one candidate. Unless and until the voter confirms his/her voting the process cannot be completed (Figure 4).

However if the casted vote is cancelled by the voter, the respective person is allowed to recast his/her vote. At the end of the day when voting process is completed the entire database will be backed up to the system itself and also will be saved on distributed server [19].

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

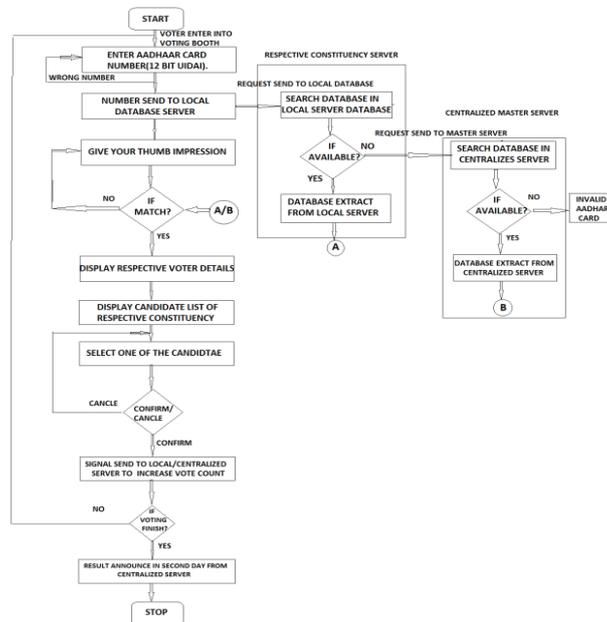


Figure 4: Flow chart of existing system.

III. DESIGN AND IMPLEMENTATION

The system is designed by considering all drawbacks and related proposed solutions. So voting system is completely implemented using raspberry pi 3 models B. Figures 5 shows the block diagram of existing system after connecting all peripherals to raspberry pi.

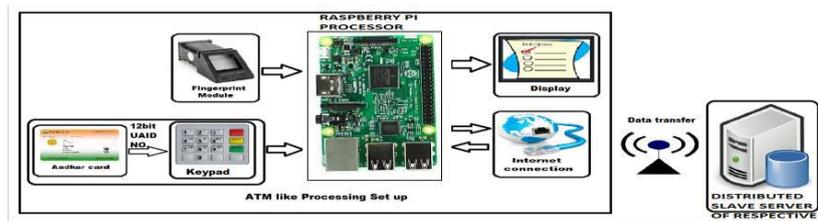


Figure 5: Block diagram of proposed system.

There are two main advantages of this existing system over electronic voting machine [20-24].

3.1 The System is Based on Biometric Authentication using Aadhaar Card

The cost of a fingerprint based biometric system is relatively low in comparison to other biometric based authentication systems like iris recognition, face readers, retina scanning, voice recognitions or hand geometry. So we used thumb impression for correctly identify the voters. Here the fingerprint module is connected to raspberry pi board through GPIO pins. First voter enter their aadhaar card number and give their thumb impression that time their Aadhaar card database is accessed from server. If accessed biometric data is matched with given data then this voter is allow for vote. Flow diagram for biometric authentication process is shown below Figure 6.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

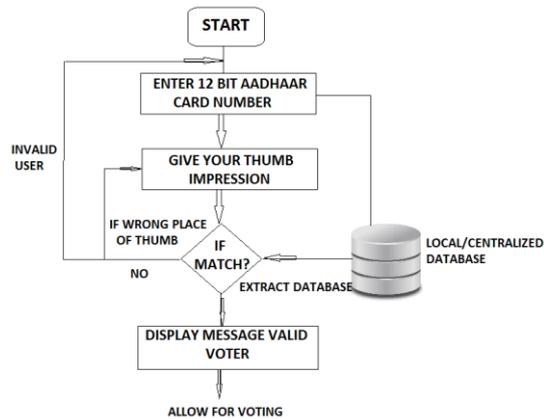


Figure 6: flow chart of authentication process.

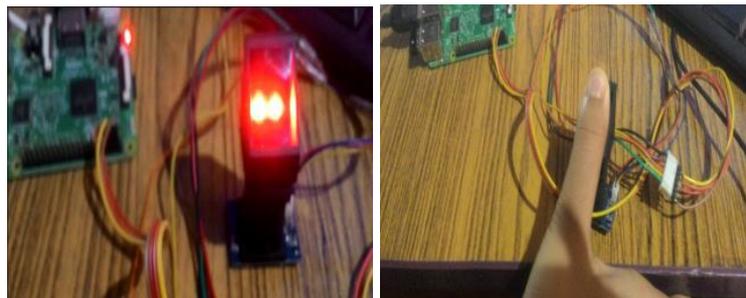


Figure 7: Thumb reader with raspberry pi 3 model B.

Above diagram shows the fingerprint module is activated after entering the Aadhaar card number then the voter put their thumb on thumb reader for authentication (Figure 7).

3.2 The System is Based on Distributed Server Architecture

Process of database accessing between master and slave server is following:

- **There are two conditions:**

- 1) If same constituency voter – If Then database access from local database which is called as slave server of respective constituency.
- 2) If other constituency voter – then database access from database of centralized master server (Figure 8).

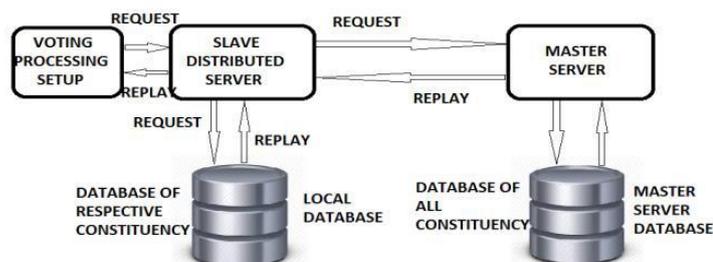


Figure 8: Database accessing process.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

Figure 9 shows the working flow of distributed servers. If voter want to cast their vote on voting booth which is present in their own constituency then their biometric data fetch from slave server which is placed at boundary of their own constituency. It is process like a cache hit means the required data is available in cache memory [25]. Second possibility is voter want to cast their vote in other constituency voting booth then they enter their 12 bit Aadhaar card number, Their data is first check into slave server of respective constituency, if data is not present in that server, this server send request to master server to access biometric data of respective voter. This problem is like cache miss means data is not present into cache memory then it needs to fetch data from main memory it is called penalty [26,27].

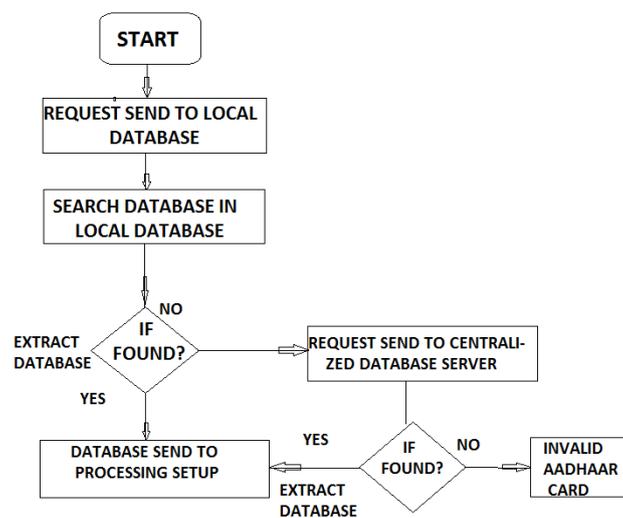


Figure 9: flow chart of database accessing in existing system.

The complete database is stored in master and slave server which is shown below Figure 10.

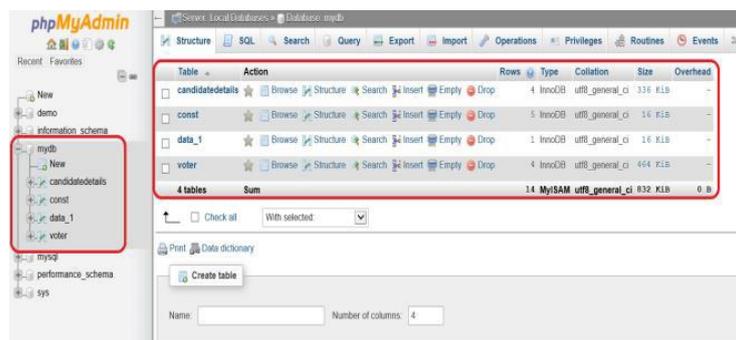


Figure 10: Database in the server.

Voter's data is stored in the server which is shown in Figure 11.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

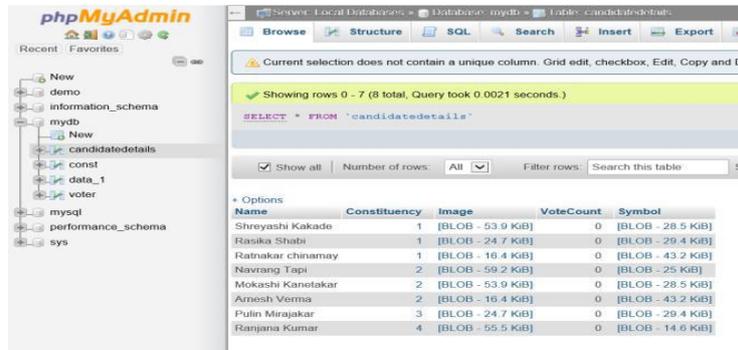


Figure 11: Candidate list stored in the server.

IV. RESULTS AND DISCUSSION

The currently used voting system is enhanced by adding the biometric authentication which results in exact identification of voters [28]. However the use of distributed server approach reduced the long distance travelling of the voters in case of change in constituency. The results that we have got are explained as follows,

The voting processes are start from entering Aadhaar card number which is shown in below Figure 12.

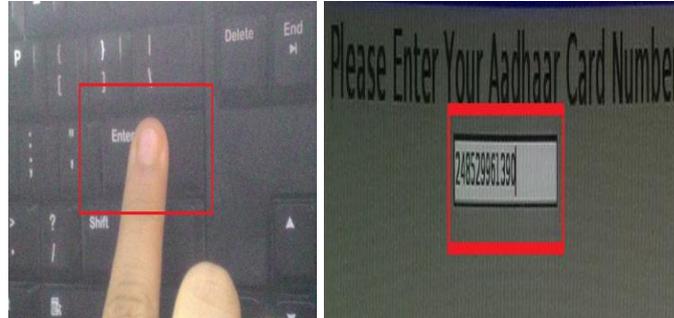


Figure 12: Entering Aadhaar card number.

After that voter give their thumb impression for authentication Figure 13.

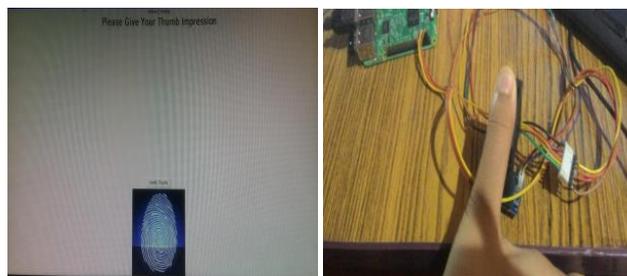


Figure 13: Authentication process with fingerprint.

If the given thumb impression is not matched with the biometric data in database or if the thumb impression is not provided in correct manner then displayed message on screen is “data error “ and “ Data not matching with database”. This is shown in Figure 7.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

4.1 User Validation Process

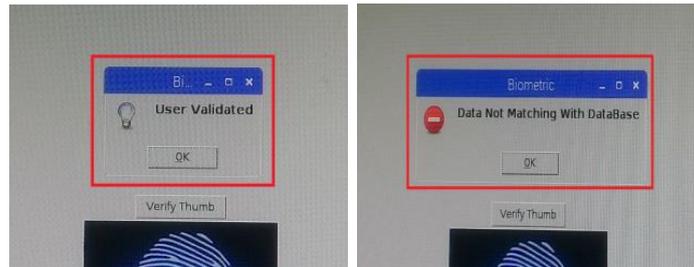


Figure 14: Validation process.

If the given thumb impression is matched with biometric data in database then displayed message on screen is “User validated” [29,30]. The voter is allowing to voting process. This is shown in Figure 14.

Respective voter profile display on screen Figure 15.

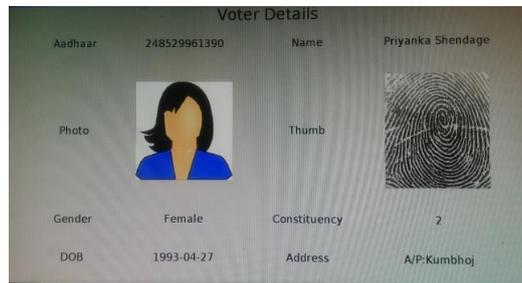


Figure 15: Voter's profile.

Candidate list is displayed on screen of respective constituency to which the voter belongs to Figure 16.

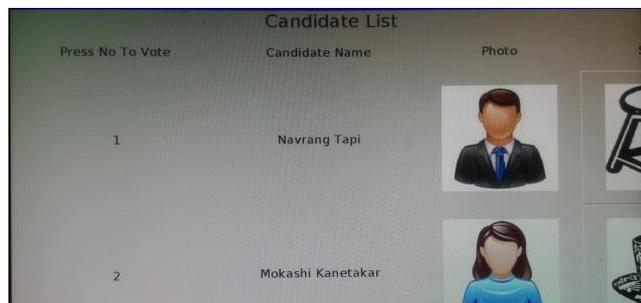


Figure 16: Candidate list.

Voter must select one of the candidate the by pressing either ‘1’ or ‘2’ button on keypad. In order to confirm the casting of vote the voter is asked whether he is sure to confirm his vote with the message “Are you sure?”

If “yes” is pressed voting process is completed whereas if “No” is pressed the voter can still choose the other candidate. Here voting process is completed [31].

Result is updated on server which is shown in Figure 17 below,

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017



Name	Constituency	Image	VoteCount	Symbol
Shreyashi Kakade	1	[BLOB - 53.9 KiB]	0	[BLOB - 28.5 KiB]
Rasika Shabi	1	[BLOB - 24.7 KiB]	0	[BLOB - 29.4 KiB]
Ratnakar chinamay	1	[BLOB - 16.4 KiB]	0	[BLOB - 43.2 KiB]
Navrang Tapi	2	[BLOB - 59.2 KiB]	0	[BLOB - 25 KiB]
Mokashi Kanetakar	2	[BLOB - 53.9 KiB]	0	[BLOB - 28.5 KiB]
Amesh Verma	2	[BLOB - 16.4 KiB]	2	[BLOB - 43.2 KiB]
Pulin Mirajakar	3	[BLOB - 24.7 KiB]	0	[BLOB - 29.4 KiB]
Ranjana Kumar	4	[BLOB - 55.5 KiB]	0	[BLOB - 14.6 KiB]

Figure 17: Updated result on server.

Advantages of existing system over EVM:

1. Due to addition of biometric authentication the chances of fake voting is reduced.
2. Systems become reliable, flexible and transparent in nature.
3. Due to addition of distributed server architecture voter can cast their vote from anywhere in India so percentage of voting is increases.
4. Public and Transport related problems at the time of voting days are reduces.

V. CONCLUSION

The present voting system deals with number of problems such as fake voting and fraud either by implementing malpractices while voting or by doing malfunctioning with the voting machine. Due to this the undesirable and worst case candidates get elected. So to avoid this and make the process of voting transparent in nature, a system can be developed which would absolutely add to the accuracy of casting of votes and would nullify the chances of malpractices as it involves a total full proof electronic system. The system is also reliable in the sense that it can be used and implemented with ease and is flexible in nature. The main advantage of the system could be that the vote can be casted from any constituency, which is irrespective of the present location of the citizen, along with the authentication of voter with distributed server approach. The system can be used by the government of India to replace the currently used electronic voting system.

5.1 Future Discussion

In the proposed system we have used keypad for entering the Aadhaar card number of the voter. However in case of some of the illiterate voters we can make use of swipe machine for automatically detecting aadhar card number of the voter In addition to that the use of image processing with segmentation algorithm the exact identification of aadhar card number can be carried out.

VI. REFERENCE

1. S Anandaraj, R Anish, et al. Secured Electronic Voting Machine using Biometric. IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS) 2015.
2. NV Vishal, Smart-Voting using Biometric. International Journal of Emerging Technology and Advanced Engineering 2014; 4: 672-676.
3. R Chris, Biometric Technologies- fingerprint 2006: 1-23.
4. KY Virendra, B Saumya, et al. An Approach to Electronic Voting System using UIDAI. International Conference on Electronics and Communication Systems. 2014.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2017

5. K Amanpreet, K Yash, et al. Microcontroller Based Voice Activated Mobile Controlled Electronic Voting Machine. International Journal of Advanced Research in Computer and Communication Engineering 2013; 2: 1331-1333.
6. KA Ratnakar, MS Kumbhar, An Identity- Authentication System Using Fingerprints. Journal of Engineering Research and Applications (IJERA) 2012; 2: 303-311.
7. DK Ashok, TU Sariba Begum, A Novel design of Electronic Voting System Using Fingerprint. International Journal of innovative technology and creative engineering 2011; 1: 12-19.
8. Introducing Electronic Voting: Essential Considerations International Institute for Democracy and Electoral Assistance December 2011.
9. PK Hari, J Alex Halderman, et al. Security Analysis of India's Electronic Voting Machines. EVM India 2010.
10. JK Anil, R Arun, et al. Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology 2004; 14: 4-20.
11. S Prabhakar, S Pankanti, et al. Biometric recognition: Security and privacy concerns. IEEE Security and Privacy 2003; 99: 33-42.
12. A Andrew, Rafail Ostrovsky. Fingerprint Recognition 2002.
13. Election Commission of India. Subject: Supreme Court's order dated 2nd May, 2002 relating to right to information of electors regarding criminal antecedents, assets and liabilities and educational qualifications of candidates – implementation of the order. 2002.
14. R Prateek, PR Keerthi. A study of fingerprints in relation to gender and blood group. Journal of Indian Academy of Forensic Medicine 2010; 32: 11-14.
15. Ed Arnold, History of Voting Systems in California. Bill Jones Secretary of State 1999.
16. JP Gibson, K Robert, et al. A review of E-voting: the past, present and future. Annals of Telecommunication 2016.
17. https://en.wikipedia.org/wiki/Unique_Identification_Authority_of_India. Unique Identification Authority of India
18. W Scott, W Eric, et al. Security analysis of India's electronic voting machines. SCRIBD 2010; 1-14.
19. PP Shendage, PC Bhaskar, Distributed Server Approach for Novel E-Voting System with Biometric Authentication Using Aadhaar Card. International Journal for Scientific Research & Development 2017; 5: 1593-1597.
20. L Philipp, H Rolf, Verifiable Internet Elections with Everlasting Privacy and Minimal Trust. International Conference on E-Voting and Identity 2015; 74-91.
21. B Jurlind, R Karen, et al. An investigation into the usability of electronic voting systems for complex elections. Center for research in security and privacy 2016.
22. BK Balkrushna, SS Shahebaz, et al. A Survey on Smart E-Voting System Based On Fingerprint Recognition 2015.
23. S Soumadip, S Sankhadip, Automatic Voting Machine – An Advanced Model for Secured Biometrics Based Voting System. International Journal on Recent and Innovation Trends in Computing and Communication 2015; 3: 4586-4594.
24. S Martine, A Survey of Modern Electronic Voting Technologies. Norwegian University of Science and Technology Department of Telematics 2010.
25. K Smita, K Reena, Survey on Secure Online Voting System. International Journal of Computer Applications 2016; 134: 19-21.
26. D Ashok Kumar, T Ummal Sariba Begum, Electronic voting machine - A review. International Conference on Pattern Recognition, Informatics and Medical Engineering 2012.
27. PK Hari, J Alex Halderman, et al. Security Analysis of India's Electronic Voting Machines. India EVM 2010.
28. D Anooshmita, Usability of electronic voting system in India and innovatory approach. Int. Journal of Applied Sciences and Engineering Research 2015; 4.
29. L David, Component Based Electronic Voting Systems.
30. OO Okediran, EO Omidiora, et al. A Framework for a Multifaceted Electronic Voting System. International Journal of Applied Science and Technology. 2011; 1: 135-142.
31. K Aggelos, K Michael, et al. An Internet Voting System Supporting User Privacy. Computer Security Applications 2006; 165-174.