Fingerprint Based e-Voting System using Aadhar Database

Rohan Patel[1], Vaibhav Ghorpade[2], Vinay Jain[3] and Mansi Kambli[4]

Computer Department, K. J. Somaiya College of Engineering, Mumbai, India.

[1]rohan.patel@somaiya.edu

[2]vaibhav.g@somaiya.edu

[3]vinay.jain@somaiya.edu

[4]prasadinipadwal@somaiya.edu

ABSTRACT

This project proposes a secure online e-voting system that uses UIDAI or aadhar database as its backend. The system ensures authentication of an individual by matching fingerprints and eligibility is checked by calculating the age of the voter thus making the existing voting cards redundant. The proposed system can handle voting at different levels such as Parliamentary, Municipality, State legislative assembly, etc simultaneously. The project will bring transparency in the voting process by assuring the voters that their votes will be in favor of the candidates of their choice. Besides electronic recording and counting of votes will be faster, more accurate and less labor intensive. The design of this system will make voting process more convenient and may therefore lead to improve the turnout.

Keywords-e-Voting, Fingerprint, Aadhar, Uidai.

1. INTRODUCTION

In paper-based elections voters cast their votes by simply depositing their ballots in sealed boxes distributed across the electoral circuits around a given country. When the election period ends, all these boxes are opened and votes are counted manually in presence of the certified officials. In this process there can be error in counting of votes or in some cases voters find ways to vote more than once. Sometimes votes are even manipulated to distort the results of an election in favor of certain candidates [1]. In order to avoid these shortcomings the government of India came up with Direct-recording electronic (DRE) voting system which are usually referred as Electronic Voting Machines or EVMs. These devices have been praised for their simple design, ease of use and reliability. However it has been found that EVMs are not tamper proof and are easily hackable. Moreover this attacks, hardware as well as software, go without any detection but are quite simple to implement. Hari K. Prasad and fellow researchers simulated attacks to demonstrate how secure EVMs really are [2].This made us to bring forth a system that is secure, transparent, reliable as well

as easy to use for the citizens. Biometric e-voting systems are not a phenomenon anymore they are being actively used in countries like Ghana and Ireland and are spreading to many other developing nations.[4,5] In this project we propose an integration of the CIDR with that of e-voting mechanism to make e-voting in India a reality.

2. PROPOSED SYSTEM

2.1 Components of the System

We propose client-server web-enabled software architecture for the project. On the client side we have a fingerprint scanner and a GUI that accepts voter's aadhar number, provides an interface to vote and display confirmation, status and error messages. The GUIs will only act on events from the server and feedback of the voter without any extra processing.

Servers are placed at remote locations from the poll booths. They are used for carrying out all the processing work such as image processing, transferring data between the client and the database, generating statistics, sending messages to voters, etc.

There is a central database called Central Identities Data Repository or CIDR which forms the backbone of this system. It contains all the demographic and biometric data of every citizen of India. In order to reduce load on the central database there are zonal databases that will be located alongside the servers which will contain cached copies of data of the inhabitants that fall under its zone. These zones are decided on the basis of population density, area and other factors. All the zonal databases retrieve data from CIDR of only those people who come under its scope. This data is periodically updated and is stored in volatile form so that it can be erased if and when necessary such as during security attacks, natural calamities, maintenance works, etc. The zonal databases will retrieve only the data that is pertaining to the voting process and exclude all other irrelevant information. These databases will be used for generating statistics and results of the electoral process. These databases make it possible to allow voting from anywhere provided that the voter is within electoral circuits.
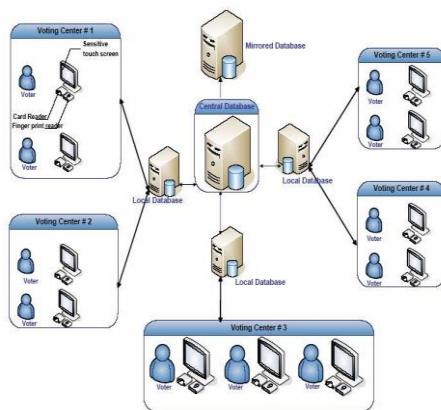

Figure 1: Architecture of the Proposed System

2.3 Authentication and Verification of the Voter

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In order to authenticate a person we require them to have a valid UID number. The number will be checked in the local database records first. If it is not found then it will search the central repository. It involves one-to-many match. If the person's number is not found in the central database then of course s/he will be devoid of taking part in the voting process. On the other hand if the number is present in the central database then the data of that person will be cached to the zonal database. This record is extracted from the local database and sent to authenticating servers for further processing.

For verification the person's fingerprint will be scanned at the client-side and matched one-to-one at the servers with the data extracted from the local database. This process puts less stress on the local database and improves data traffic.

We use fingerprints for authentication because processing fingerprints is faster and better than other biometric data. Moreover aadhar details would be insufficient to establish the true identity of a person since they can be easily faked but by using fingerprints it is ensured that such fake entries are blocked right at the very beginning.

2.4 Preventing Fraudulent Voting

The first and the foremost thing to ensure proper voting is by accurately authenticating every voter. It is necessary to identify that every person coming to vote is unique otherwise it will violate the very principle of voting. Any person would be voting on behalf of others. Fingerprint matching ensures the authentication that the system requires. However in order to improve accuracy it is important to keep false reject rate (FRR) and false accept rate (FAR) as low as possible; practically close to zero. This can be achieved by using best finger method. Using 2 best fingers can improve the accuracy to 98% (FRR-2%) with a single attempt and above 99 % (FRR – 1%) with up to 3-attempts.[3] Specifications of fingerprints and relevant details are provided in [6].

To prevent underage individuals from voting, the system calculates person's age from the birth date present in the database records. If the calculated age is above permissible limit the person is allowed to vote and prevented otherwise. Fig. 2 describes the flowchart of the system.

To prevent voters from voting two or multiple times we implement voting flags in the local databases. This flag is initially set to false. After the voter has cast the vote, his/her vote flag will be set to true. This will prevent the same person from voting again. These flags are temporary and can be reset after the election has completed so that the voter can participate in the next election.

Providing transparency is another form of preventing malpractices in voting process from a voter's point of view. Since a voter has to put his trust into computer's hardware and software that processes the vote, it doesn't actually guarantee transparency in truest sense. Thus, we came up with a solution to build the voter's trust on the system by sending a message to

the voters registered mobile stating that s/he has successfully voted with the corresponding aadhar number at a specified time.

2.5 Generating Reports

Whenever a voter casts a vote in favor of the candidate of choice, the vote count of that candidate gets incremented in the local database. The votes from all the local databases are summed up to get the final figure that the candidate has received. Thus this system provides instantaneous results and prevents unnecessary use of manpower and wastage of time.

Since this is an electronic system and uses digital data it has several advantages. Statistics can be generated from the obtained data for e.g. we could answer how many people have voted from a certain region, how many females voted, which age group voted the most, the highest turnouts, comparisons from previous years, etc. all that was not possible from traditional voting methods not even from EVMs. It would provide important insights into the election results and help improve the system even further.
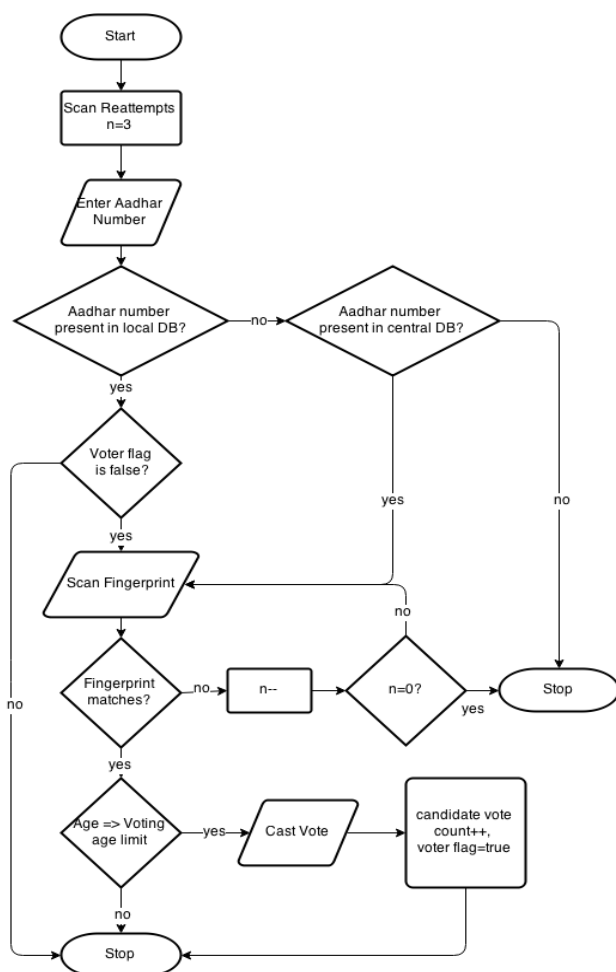

Figure 2: System Flowchart

3. CONCLUSION

In this paper, we have proposed an online voting system which is better and faster than previous systems. The new system prevents access to illegal voters, provides ease of use, transparency and maintains integrity of the voting process. The system also prevents multiple votes by the same person and checks eligibility of the voter. It also allows a person to vote from anywhere provided that the voter is within electoral limits.

4. LIMITATIONS

E-voting systems have many advantages over conventional systems but it still has to solve many hurdles before becoming coming to fruition. India's majority population is rural and illiterate. Also there is shortage of power and inadequate network between cities and villages which further adds to the problems. This system requires good bandwidth and high speed internet connection for operating, but it is still a distant reality in many cities in India. However conditions are improving with the onset of education in rural areas and with increasing urban population this project may soon become a reality.

ACKNOWLEDGMENT

REFERENCES

[1] 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.

[2] Prasad, H. K., Halderman, A. J., & Gonggrijp, R. (Oct. 2010). Security Analysis of India's Electronic Voting Machines. Proc. 17th ACM Conference on Computer and Communications Security (CCS '10).

[3] UIDAI. (2012). Role of Biometric Technology in Aadhaar Authentication.

[4] Yinyeh, M. O., & Gbolagade, K. A. (2013). Overview of Biometric Electronic Voting System in Ghana. International Journal of Advanced Research in Computer Science and Software Engineering.

[5] McGaley, Margaret. "Irish Citizens for Trustworthy Voting." 6 July 2004. http://evoting.cs.may.ie/

[6] UIDAI, Biometrics Design Standards For UID Applications, 2009

.