Online Voting System Using Aadhar Card Database and Fingerprint Scanner

T. H. Feiroz Khan[1], Siddharth Srivastava[2], Anurag Thakur[3], Antony John Martin[4]
[1]Assistant Professor, Department of Computer Science and Engineering, SRMIST, Chennai, India
[2,3,4]Student, Department of Computer Science and Engineering, SRMIST, Chennai, India

***Abstract*—The main thesis of this project is to develop a secure Electronic voting machine using Finger print identification method, for finger print accessing we use AADHAR card database. At the time of voting in the elections, the e -voting process authentication can be done using finger vein sensing, which enables the electronic ballot reset for allowing voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Administration unit in a timely manner using Zigbee System with cryptography technique. Online polling system is the system which enables user to vote online. The Voting system consisted of server services which are each linked with a database for storing data. Voters can also use the services to log into the electronic voting system website. The voter information and their voting's information will be maintained by aadhar card data base. Admin will maintain all information regarding voter and counts automatically their voting. Voting system takes finger print and face image as password.**

***Index Terms*—constitutional amendments, Finger print matching and authentication**

I. Introduction

The objective of voting is to allow voters to exercise their right to express their choices regarding specific issues, pieces of leg isolation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political representatives. Technology is being used more and more as a tool to assist voters to cast their votes. To allow the exercise of this right, almost all voting systems around the world include the following steps: voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results. Voter identification is required during two phases of the electoral process: first for voter registration in order to establish the right to vote and afterwards, at voting time, to allow a citizen to exercise their right to vote by verifying if the person satisfies all the requirements needed to vote (authentication).

II. 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. 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.

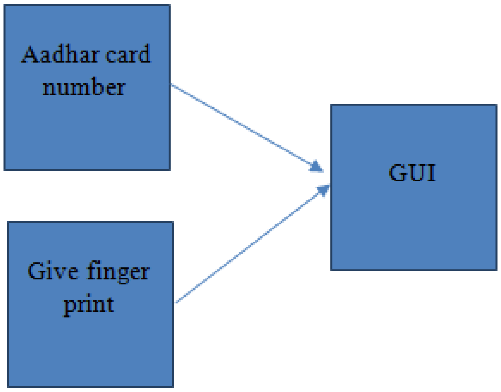

Fig. 1. Components of the system

III. Preventing Fraudulent Voting

The first and the leading thing to guarantee proper voting is by accurately validating every voter. It is essential 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. 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. To prevent voters from voting two or multiple times we implement voting flags in the local databases. This flag is initially set to false.

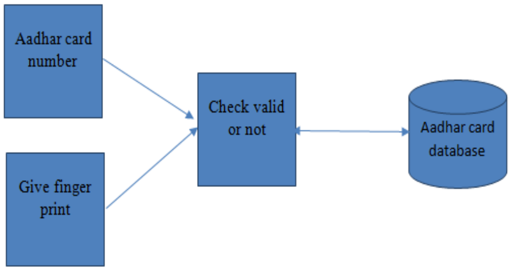

Fig. 2. Preventing fraudulent voting

IV. 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.

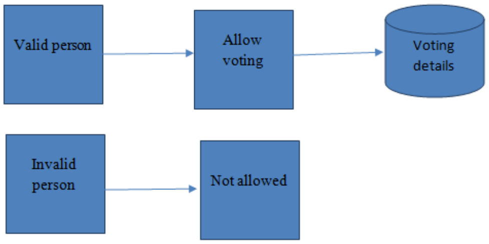

Fig. 3. Authentication and verification of voter

V. 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.

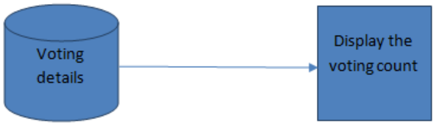

Fig. 4. Generating reports

VI. System Architecture

Design is a multi- step that focuses on data structure software architecture, procedural details, algorithm and interface between modules. The design process also translates the requirements into presentation of software that can be accessed for quality before coding begins. Computer software design change continuously as new methods; better analysis and border understanding evolved. Software design is at relatively early stage in its revolution. Therefore, software design methodology lacks the depth, flexibility and quantitative nature that are normally associated with more classical engineering disciplines. However techniques for software designs do exit, criteria for design qualities are available and design notation can be applied.

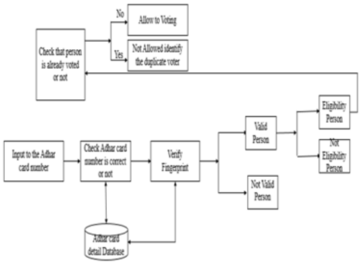
Check that person is already voted or not
No
Allow to Voting
Yes
Not Allowed identify the duplicate voter
Input to the Adhar card number
Check Adhar card number is correct or not
Verify Fingerprint
Valid Person
Not Valid Person
Eligibility Person
Not Eligibility Person
Adhar card detail Database

Fig. 5. System architecture

VII. System Design

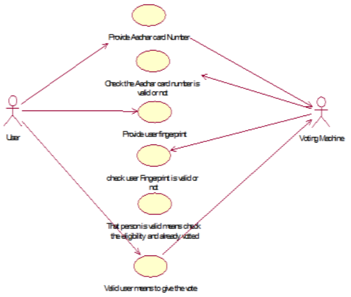
Provide Aadhar card Number
Check the Aadhar card number is valid or not
Provide user fingerprint
check user Fingerprint is valid or not
That person is valid means check the eligibility and already votted
Valid user means to give the vote
User
Voting Machine

Fig. 6. System design

VIII. Collaboration Diagram

A collaboration diagram, also called a communication diagram or interaction diagram, is an illustration of the relationships and interactions among software objects in the

Unified Modeling Language (UML). The concept is more than a decade old although it has been refined as modeling paradigms have evolved.

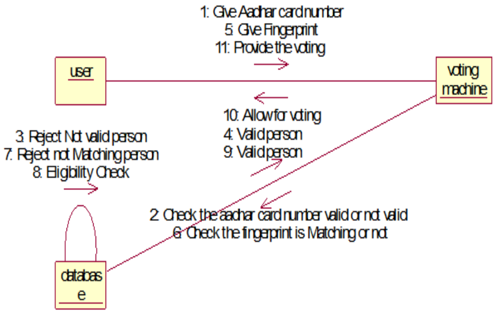
1: Give Aadhar card number
5: Give Fingerprint
11: Provide the voting
user
voting machine
10: Allow for voting
4: Valid person
9: Valid person
3: Reject Not valid person
7: Reject not Matching person
8: Eligibility Check
2: Check the aadhar card number valid or not valid
6: Check the fingerprint is Matching or not
database

Fig. 7. Collaboration diagram

IX. Data Flow Diagram

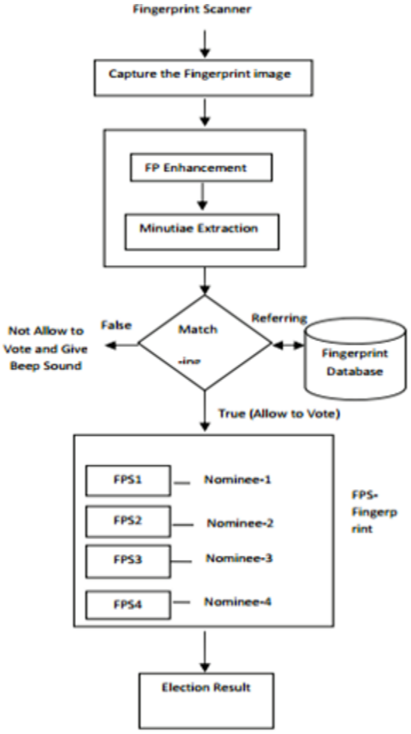

Fig. 8. Data flow diagram

X. Future Scope

Future enhancements focused to design a system which can be easy to use and provide security and privacy of votes on acceptable level by concentrating the authentication and processing section

XI. 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.

References

[1] D. Ashok Kumar, T. Ummal Sariba Begum A Novel design of Electronic Voting System Using Fingerprint International Journal of Innovative Technology & Creative Engineering (Issn: 2045-8711) Vol.1 No.1 January 2011.

[2] .Barbara Ondrisck E-Voting System Security Optimization Proceedings of The 42nd Hawaii International Conference on System Sciences-2009

[3] Bernd Heisele,a,b, Purdy Ho, c Jane Wu,b and Tomaso Poggiob Face recognition: component-based versus global approaches," Transactions On Software Engineering, Vol. 36, No. 4, July/August 2010.

[4] Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard A Kemmerer, William Robertson, Fredrik Valeur, And Giovanni Vigna, An Experience In Testing The Security Of Real-World Electronic Voting System.

[5] Kashif Hussain Memon, Dileep Kumar and Syed Muhammad Usman, Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method 2011 International Conference On Information And Intelligent Computing IPCSIT Vol.18 (2011).

[6] Hari K. Prasad Arun Kankipati Sai Krishna Sakhamuri Vasavya Yagati Netindia, Security Analysis of India's Electronic Voting Machines Scott Wolchok Eric Wustrow J. Alex Halderman The University of Michigan Hyderabad HristinaMihajloska, Vesna Dimitrova and Ljupcho Antovski Security Aspects of Electronic Voting Systems Cyril and Methodius University Faculty of NaturalSciences and Informatics Institute of Informatics, Skopje, Macedonia 60.