Secure E-Voting and Result Verification through Cryptography

G.D.Vignesh

Department of Electronics & Communication Engineering, MVJ College of Engineering, Affiliated to VTU, Bangalore, India.

ABSTRACT

This paper depicts the procedure and working of E-casting a ballot framework which is exceedingly secure, biometric validation framework alongside date of birth (DOB) based confirmation framework to improve the casting a ballot procedure amid race. Further the vote thrown by a client is encoded before putting away in database. E-casting a ballot framework uses Aadhar number of client for ID and check of voter. With brilliant casting a ballot framework, voter can make their choice with cell phone and dodge all sort of lines at surveying stall. At first, client must punch in his Aadhar number in the E-casting ballot framework. However, a database will be created displaying te candidates above 18 years of age to know that they are eligible. The E-casting ballot framework uses the Aadhar number to validate the client through DOB which will be the password to be entered by the voter to cast a vote. The match of the DOB with the Aadhar card allows voting. Individuals without Smart telephones can cast a ballot through E-casting ballot framework with an extra advance of validation through profoundly modern Aadhar based biometric confirmation. This Voting System effectively enables individuals to cast a ballot utilizing advanced cells hence lessens the lines heaped up at surveying stall. However, the members whose votes aren't received can be displayed and action can be taken against them, to prevent people from not giving importance to voting. Likewise, it gives an exceptionally solid biometric verification system for individuals who don't need vote utilizing advanced cells in this way avert appointive extortion. [1,2,3,4]

Keywords: Cryptography, Electronic Voting Machine, Smart Voting, Vote.

1. INTRODUCTION

In a majority rules system, casting a ballot is an intend to enable constituent to pick their political agent. India since Independence has embraced Universal grown-up suffrage. When an individual is qualified to cast a ballot they can do their voter enlistment. Race Commission of India refreshes in rundown of qualified of voters for a body electorate and issues voter ID. At the season of putting the voter must go to surveying corner and demonstrate his voter ID and experts on surveying stall confirm if the name is available in the voter list. On the off chance that the voter is qualified, at that point and the person is permitted to make the choice.

Electronic casting a ballot machine is a basic electronic gadget used to include in track cast a ballot in traditional casting a ballot procedure. In spite of the fact that, EVMs conquered the issues related with framework i.e, manual counting in treatment of votes, yet issue of security and voter validation is as yet a major test. Presently EVMs don't have mechanical assembly for confirmation, along these lines it is required for specialists to physically check the id of each voter. Aside from the way that voter ID can undoubtedly be manufactured which is a major gap in security of casting a ballot procedure, different security examiners have instructed against the utilization concerning EVMs as these are helpless against hacking. The whole manual confirmation and check process makes casting a ballot procedure very tedious as the administration authorities on the surveying stall should check the ID card of the voter and match it with the rundown they have, to ensure that it is an approved card and after that empower the individual to survey his vote. Individuals must remain in lines for a long time and on the off chance that somebody isn't in the town on casting a ballot day, at that point he/she can't cast a ballot.

To maintain a strategic distance from the issues looked in ordinary casting a ballot framework, there is requirement for clever casting a ballot framework that recognizes and checks the voter's credentials online in this manner enabling them to cast a ballot from anyplace. The present work exhibits a creative casting a ballot framework, which offers hearty check and validation system. Utilizing this, individuals can cast a ballot with an application

introduced on their advanced mobile phones. It additionally enables clients to cast a ballot without advanced cells. It gives separate channels to validation and stores vote in encoded structure[6]. The further subtleties are clarified in detail proposed framework segment.

2. THE PROBLEM STATEMENT

Existing arrangement of casting a ballot has numerous issues of security and confirmation. Proposed framework gives a superior arrangement of security by utilizing biometric verification framework and also gives an office to client to make a choice utilizing cell phones. To reduce the opportunity of vote producing and maintenance cost of survey stall, a keen casting a ballot framework is presented. It displays high security through confirming a voter and furthermore keeps up the protection by encoding the made choice. It offers the office of web based casting a ballot and spares people's time while remaining in line[9,10].

3. THE PROPOSED SOLUTION

A. *The several stages for the voting procedure will be as follows*

The Database

The Aadhar card data containing every individual name, date of birth, sexual orientation, Aadhar number, E-mail ID, address, state, region, unique mark of left and right hand alongside international ID measure photograph are put into the administrator database. [5,7] From the Aadhar information, the individuals above 18 years of age are picked up as it is the qualification foundation for casting a ballot and are saved. Their DOB's will be used to match their passwords.

Information Check

To make a vote, Aadhar number is required. Aadhar card number is utilized in this framework rather than conventional voter ID which guarantees that a solitary individual wouldn't probably make more than one choice. Aadhar number is confirmed utilizing Aadhar database server and just substantial Aadhar number is permitted to make a vote.

Access

The solution provides the two following possibilities:

1. For smartphone users, DOBs as their passwords.

2. For others, fingerprint recognition

By along these lines of verification, voter does not require to introduce himself physically at the polling stall. Voter can legitimately validate himself utilizing cell phones and make a vote from anyplace. This would likewise limit the costs of government as it doesn't require any equipment gadgets. The clients should enter a secret key[8], which will be their DOBs, which will announce the singularity of the client. The secret phrase can be coordinated and access can be conceded. For other client who does not have advanced mobile phones, biometric gadget[9], unique

mark acknowledgment, can be utilized as validation as the finger impression module is very moderate as well. It utilizes the client's database server for verifying unique mark of a voter.

B. The Vote

Confirmed voter can make the choice. Cryptography is performed to scramble the code. To scramble the vote, a Key Manager like Gemalto KeySecure or a HSM (Hardware Security Module) is utilized which will create and store the key inside itself and as a rule will likewise perform encryption/decoding in its protected memory. Just approved individuals who have decoding key can decrypt it by performing decoding calculation and tally the made votes and also find the voters who failed to cast their vote.
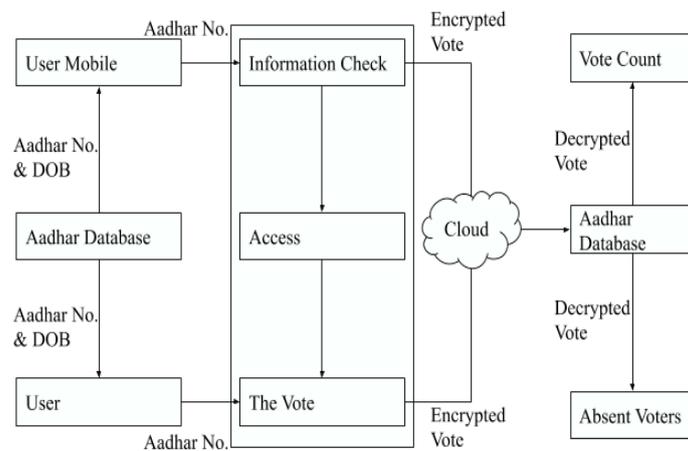

Fig. 1: The system architecture

4. THE IMPLEMENTATION PROCEDURE

- To execute this framework, Oracle 12c is utilized as the database server. What's more, the database server runs database maker to make the database required to run the framework. This instrument, makes the race and Meta databases, and populates different tables with at first required data. The database maker instrument is actualized in Java. The instrument opens a GUI to end client who can be hurried to make/erase the database when required.

- The framework utilizes Microsoft Internet Information Server (IIS) as a web server.

- The framework's GUI and different related site pages are made utilizing Java Server Pages(JSP).

- The casting a ballot data given by client through the GUI is prepared and encoded in Java layer and put away in Oracle database utilizing JDBC.

- The GSM modem is utilized to associate remote voters to the framework.

5. CONCLUSION

This framework is the cutting edge online exceedingly verified casting a ballot framework which individuals can access to execute their casting a ballot rights. The voter just needs their Aadhar card to get to the framework. The

framework incorporates all highlights of present day state EVM for considering admirably as chronicle cast a ballot. This framework additionally diminishes the extent of false appointive practices by cutting down the human intervention to its base. Notwithstanding giving a very solid validation component, it additionally gives an adaptable answer for huge decisions. The framework will unquestionably build the casting a ballot rate by permitting individuals living in remote to cast a ballot and furthermore because of the dread of move which may be made against them. Likewise, it will chop down the time and asset utilization amid decision in contrast with its regular partners.

6. ACKNOWLEDGMENT

REFERENCES

[1] S B Khairmar, P S Naidu and R Kharat, "Secure authentication for online voting system", 2016 International Conference on Computing Communication Control and automation (ICCUBEA), Pune, 2016, pp. 1-4.

[2] Bhuvanapriya R, Rozil Banu S, Sivapriya P and Kalaiselvi V K G, "Smart Voting", 2017 2nd International Conference on Computing and Communication Technologies (ICCCT), Chennai , 2017, pp. 143-147.

[3] N Sultan, F A Barbhuiya and N Sarma, "Pai Voting: A secure online voting scheme using Pairing-Based Cryptography and Fuzzy Extractor", 2015 IEEE International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-7.

[4] S Sridharan, "Implementation of authenticated and secure online voting system," 2013, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-7.

[5] H Agarwal and G N Pandey, "Online voting system for India based on AADHAAR ID", 2013, Eleventh International Conference on ICT and Knowledge Engineering, Bangkok, 2013, pp. 1-4.

[6] L Rura, B Issac and M K Haldar, "Online voting verification with cryptography and steganography approaches", Proceedings of 2011 International Conference on Computer Science and Network Technology, Harbin, 2011, pp. 3239-3240.

[7] Vishal, V Chinmay, R Garg and P Yadav, "Online voting system linked with AADHAR", 2016, 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 125-129.

[8] Ashwini Walake, Prof. Ms. Pallavi Chavan, "Efficient Voting system with Secret Sharing Based Authentication", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6(1), 2015, 410-412.

[9] S Katuyar, K R Meka, F A Barbhuiya and S Nandi, "Online Voting System Powered by Biometric Security Using Steganography", Second International Conference on Emerging Applications of Information Technology, Kolkata, 2011, pp. 288-291.

[10] Sunita Patil, Amish Bansal, Vaibhavi Pujari, Utkarsh Raina, Roushan Kumar, "E-Smart Voting System with Secure Data Identification using Cryptography", 2018 3rd International Conference for Convergence in Technology (I2CT), Pune.

[11] K. Kim, and D. Hong, "Electronic Voting System using Mobile Terminal", World Academy of Science, Engineering and Technology, 2007, pp. 33-37.