"E voting using Cryptography"

Subodh Sandeep Wagh

Research Scholar, Marathwada Mitra Mandal's College of Engineering, Pune.

Abstract

Currently voting process throughout the world is done using Electronic Voting Machines. Though this system is widely followed, there are many drawbacks of the system. People have to travel to their assigned poll booth stations, wait in long queues to cast their vote, face unnecessary problems and so on. It becomes difficult for working profession people or elderly/ sick people to cast their vote due to this system. This calls for a change in system which can be done if voting processes in conducted online. Few developed countries are trying to implement online voting system on small scale and have been successful in doing so. We propose a system which overcomes limitations of existing online system which uses bio-metric technologies and instead use One Time Password system which is more secure and accurate.

Keywords: Face detection, OTP ,. bio metric, time-synchronized.

Introduction

Online voting system is a web based application. Online voting system is an online voting technique in which people who are Indian citizens and age is above 18 years and are of any sex can cast their vote without going to any physical polling station. Online voting system is a software application through which a voter can cast votes by filling forms themselves which are distributed in their respective ward. All the information in forms which has to be entered by data entry operators is stored in database. Each voter has to enter his all basic information like name, sex, religion, nationality, criminal record etc. correctly in form taken from ward. Online voting system project is implemented in java platform using Mysql database as back end. Main aim of online voting system is to develop an online application like online reservation system, for citizens who are above 18 years of age to vote through online. Using these system citizens of India can vote through online without visiting polling booth. A centralized database is maintained by election commission of India where citizens information is maintained whenever citizen is using online voting system his/her information is authenticated with the data present in database if user is not in the list he cannot use online voting system.

Users are provided with a online registration form before voting user should fill online form and submit details these details are compared with details in database and if they match then user is provided with username and password using this information user can login and vote. If conditions are not correct entry will be canceled. Also given voter ID .when registration of user is completed user gets sms with his aadhar ID and voter ID.

Existing System Problems

There are many types of problems with EVM which is currently in use they are:

1. Accuracy: It is not possible for a vote to be altered eliminated the invalid vote cannot be counted from the finally tally.

2. Democracy: It permits only eligible voters to vote and, it ensures that eligible voters vote only once. 3. Security Problems: One can change the program installed in the EVM and tamper the results after the polling by replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favor of a chosen candidate. These instructions can be sent wirelessly from a mobile phone.

4. Illegal Voting (Rigging): The very commonly known problem rigging which is faced in every electoral procedure. One candidate cast the votes of all the members or few amounts of members in the electoral list illegally. This results in the loss of votes for the other candidates participating and also increases the number votes to the candidate who performs this action. This can be done externally at the time of voting.

5. Privacy: Neither authority nor anyone else can link any ballot to the voter.

6. Verifiability: Independently verification of that all votes have been counted correctly.

7. Resistance: No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting.

8. Availability: The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll.

9. Resume Ability: The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands. The existing elections were done in traditional way, using ballot, ink and tallying the votes later. But the proposed system prevents the election from being accurate.

Existing System

The average election turnout over all nine phases for 2014 Lok Sabha election was around online is a possible idea. India's mobile phone subscriber base crested the 1 billion user's mark, as per data released recently by the country's telecom regulator. People of all age group must willingly exercise their right to vote without feeling any sort of dissatisfaction. Currently 42 percent of internet users in India have an average internet connection speed of above 4 Mbit/s, 19 percent have a speed of over 10 Mbit/s, and 10 percent enjoy speeds over 15 Mbit/s. The average internet connection speed on mobile networks in India was 4.9 Mbit/s. Online Voting overcomes various other problems faced during election process such as creating awareness among rural areas and youths, cost reduction, security, etc.

Literature Survey

1. Advance Online Voting System by Pallavi Divya, Piyush Aggarwal, Sanjay Ojha (School Of Management, Center For Development of Advanced Computing (CDAC), Noida

In this paper authors propose an approach for e actively user-friendly application for all users. This system is being developed for use by everyone with a simple and self-explanatory graphical user interface (GUI). The GUI at the server's end enables creating the polls on behalf of the client.

2. Online Election Voting Using One Time Password by Prof. Uttam Patil, Asst.Prof. at Dr.MSSCET. Computer Science branch Vaibhav More,Mahesh Patil ,8th Sem at Dr.MSSCET. Computer Science branch.

Authentication technique proposed is - One Time Password (OTP). One Time Password principle produces pseudorandom password each time the user tries to log on. This OTP will be send to voters mobile phone. An OTP is a password that is only valid for single login session thus improving the security. The system takes care that no voter can determine for whom anyone else voted and no voter can duplicate anyone elses vote.This technique is imposed to ensure that only the valid person is allowed to vote in the elections.

3. Electronic Voting System Using Aadhar Card byC. Tamizhvanan, S. Chandramohan, A. Mohamed Navfar, P. Pravin Kumar, R. Vinoth Assistant Professor, B.Tech Student Department of Electronics and Communication

Engineering Achariya College of Engineering Technology, Puducherry, India Electronic voting system provides improved features of voting system over traditional voting system such as accuracy, convenience, edibility, etc. The design of the system guarantees that no votes in favor of a given candidate are lost, due to improper tallying of the voting counts.

4. Direct Recording Electronic(DRE) voting system by S.Hashimi, S. Komatineni, and D. MacLean, it records votes by means of an electronic display provided with mechanical or electro-optical components that can be activated by the voter, that processes voter selections by means of a computer program, and that records that processed voting data in memory components.

5. Shafii Muhammad Abdulhamid et al developed an electronic voting system, which will solve manipulation of results to its barest minimum, this problem is mostly associated with the manual system of voting. The implementation of electronic voting system in Nigeria will boost the integrity of INEC and the result they produce. The programs used to develop this system are PHP, MySQL, Java Query, CSS and HTML.

6. Sahibzada Muhammad Ali et al proposed a "MicroController Based Smart Electronic Voting Machine System" which uses mechanical or electro-optical component like touch screen to provide ballot display. This machine was programmed to record voting data and then tabulates the voting data.

7. Madan Mohan Reddy et al proposed a method for voting purpose. One more advantage of this paper is, if an alcoholic person enters into polling booth, buzzer will alert authorized persons or constables who are in election duty. Because of Alcoholic sensor, we can provide peaceful environment at polling booth. If an unauthorized person enters into polling booth to cast his vote, buzzer will alert booth level officer. If already vote casted person enters into booth with his RFID tag for 2nd time voting, then also buzzer will alert booth level officer.

Proposed Work

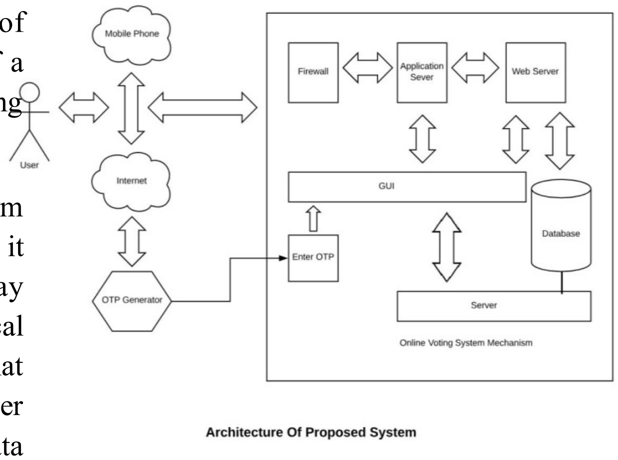
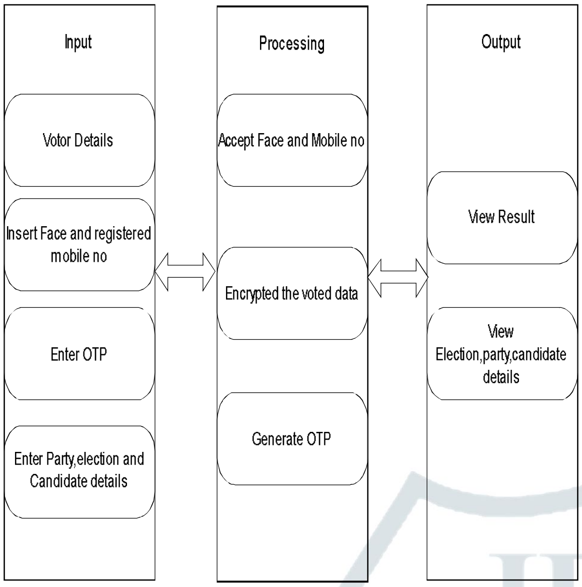


Fig 1: Architecture Diagram

The above diagram shows that the voter needs an active mobile network and internet connection to start interacting with the system. Once the voter logs in using any of the latest browsers i.e. Chrome, Firefox or Internet Explorer, the recall of system protects the voter. A recall is a system designed to prevent unauthorized access to or from a private computer network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. The interactive GUI will help users navigate through system. For logging in the system, the voter has entered all the valid credentials, and then only he/she can access other features of system. All the details are checked on database which is connected to server. For voter to cast vote, he/ she has to enter Election ID, first name, password and mobile number. If all entries are correct, then Generate OTP button will show. On clicking it an OTP of 4 or 6 digits will be sent to users mobile number, which when entered will allow voter to cast vote.

Block Diagram


Input
Votor Details
Insert Face and registered mobile no
Enter OTP
Enter Party,election and Candidate details
Processing
Accept Face and Mobile no
Encrypted the voted data
Generate OTP
Output
View Result
View Election,party,candidate details

5.1 Overview

A Smart Voting System (SVS) is a highly secured, biometric authentication system along with OTP based verification system which is used to improve the voting process during election. Further the vote casted by a user is encrypted before storing in database. SVS utilizes Aadhar number of users for identification and verification of voter. With smart voting system, voter can cast their vote with mobile phone and avoid all kind of queues at polling booth. At first the user must punch in his Aadhar number in the SVS, it then utilizes the Aadhar number to authenticate the user through OTP which will be received on their registered Aadhar linked mobile number. People without Smart phones can vote through SVS with an additional step of authentication through highly sophisticated Aadhar based biometric authentication. Smart Voting System successfully allows people to vote using smart phones thus reduces the queues piled up at polling booth. Also, it provides a highly reliable biometric authentication mechanism for people who do not want vote using smart phones thus prevent electoral fraud.

Algorithm

OTP

A one-time password or pin (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN). The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

OTP Generation OTP generation algorithms usually make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details.

Various approaches for the generation of OTPs are listed below:

A time-synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). It might look like a small calculator or a keychain charm, with an LCD that shows a number that changes occasionally. Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key. This token may be a proprietary device, or a mobile phone or similar mobile device which runs software that is proprietary, freeware, or open-source. An example of time-synchronized OTP standard is Time-based One-time Password Algorithm (TOTP). Example of this technology is the new security key that Google has started to use for last couple of years.

7.3 Methodologies

The online voting system will be having many people/ users interacting with it. These mainly consist of voters/ citizens, administrators and candidates. Let us discuss these users in brief-

1. Voters/ Citizens

This user class will consist mainly of all the people who are eligible for voting i.e. citizens above 18 years of age and have election id sanctioned by Election Commission Of India. The voters will login the system using their registered details and will be able to cast the vote. the voters will also be able to view their profiles that are uploaded on the website.

2. Administrator

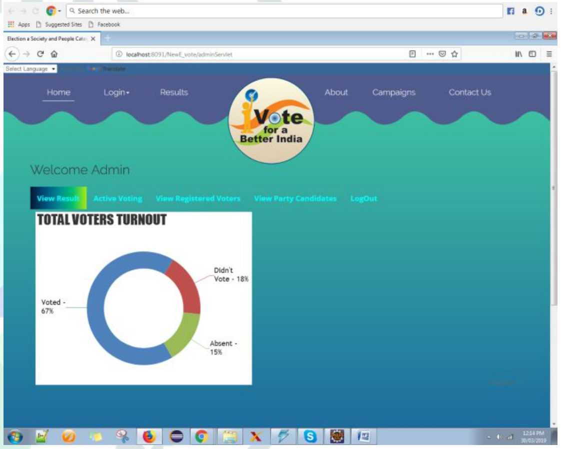
This user class will mainly consist of all the admins that are chosen by the Election Commission Of India (ECI). The admin will have privileges like adding new voter, candidates, etc. or discarding any voter/ candidate if any discrepancies are found in the data filled by them. The admin will have a different username, id and pass key assigned to them by ECI. Once logged in the admin can monitor the voting process, generate result and aslo start/ stop the voting process at given time.

3. Candidate

This user class will consist mainly of all the candidates that are contesting from their respective or allotted wards/ areas. It will contain details such as candidate name, his/ her party, education details, criminal records, address and contact number of their office, etc.

RESULTS AND DISCUSSION

The results module provide the voter with summary numbers of the voters who voted and those who did not vote on the particular posts, compute the percentage, generate the graph and finally printed the report.



Conclusion

This Online Voting system will manage the Voters information by which voter can login and use his voting rights. The system will incorporate all features of Voting system. Its provide the tools for maintaining voters vote to every party and it count total no. of votes of every party. There is a DATABASE which is maintained by the ELECTION COMMISSION OF INDIA in which all the names of voter with complete information is stored.

In this the user, who is above 18 years register his/her information in the database by filling the form available in ward numbers and when he/she want to vote he/she has to login by his/ her id and password and can vote to any party only single time. Voting detail store in database and the result is displayed by calculation. By online voting system percentage of voting is increases. It decreases the cost and time of voting process. It is very easy to use and It is vary less time consuming. It is very easy to debug.

Future Scope

In future when every part of nation will be having good internet and mobile network coverage, then older system can be scrapped and this system can be implemented. Also if number of people having smart phones increases, then an application can be developed by which voter can vote directly from his/ her Smartphone. The GUI in current system is in English only. In next development, local languages can be added making even less literate people understand and use the system.

Reference

[1] Pallavi Divya, Piyush Aggarwal, Sanjay Ojha (School Of Management, Center For Development of Advanced Computing (CDAC), Noida , ADVANCED ONLINE VOTING SYSTEM, International Journal of Scientific Research Engineering Technology (IJSRET) Volume 2 Issue 10 pp 687-691 January 2014 www.ijsret.org ISSN 2278 0882.s

[2] C.Tamizhvanan, S.Chandramohan, A. Mohamed Navfar, P.Pravin Kumar, R.Vinoth Assistant Professor1, B.Tech Student Department of Electronics and Communication Engineering Achariya College of Engineering Technology, Puducherry, India , Electronic Voting System Using Aadhaar Card, International Journal of Engineering Science and Computing, March 2018

[3] Prof. Uttam Patil, Asst.Prof. at Dr.MSSCET. Computer Science branch Vaibhav More, Mahesh Patil ,8th Sem at Dr.MSSCET. Computer Science branch, Online Election Voting Using One Time Password , National Conference on Product Design (NCPD 2016), July 2016

[4] N.Ansari, P. Sakarindr, E. Haghani, C. Zhang, A.K. Jain, and Y.Q.Shi, “Evaluating electronic voting systems equipped with voter verified paper records” , IEEE Security and Privacy, vol. 6, no.3, May 2008.

[5] Shafi’í Muhammad Abdulhamid, Damian Oshomah Ugiomoh, Mohammed Danlami Abdul Malik, (May 2013), The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity.

[6] Sahibzada Muhammad Ali, Chaudhary Arshad Mehmood, Ahsan Khawja,Rahat Nasim, Muhammad Jawad,Saeeda Usman, Sikandar Khan, Saqib Salahuddin, Mian Atif Ihsan. “Micro Controller Based Smart Electronic Voting Machine System”2014 IEEE.

[7] B. Madan Mohan Reddy, D. Srihari, (April 2015), RFID Based Biometric Voting Machine Linked to Aadhaar for Safe and Secure Voting.