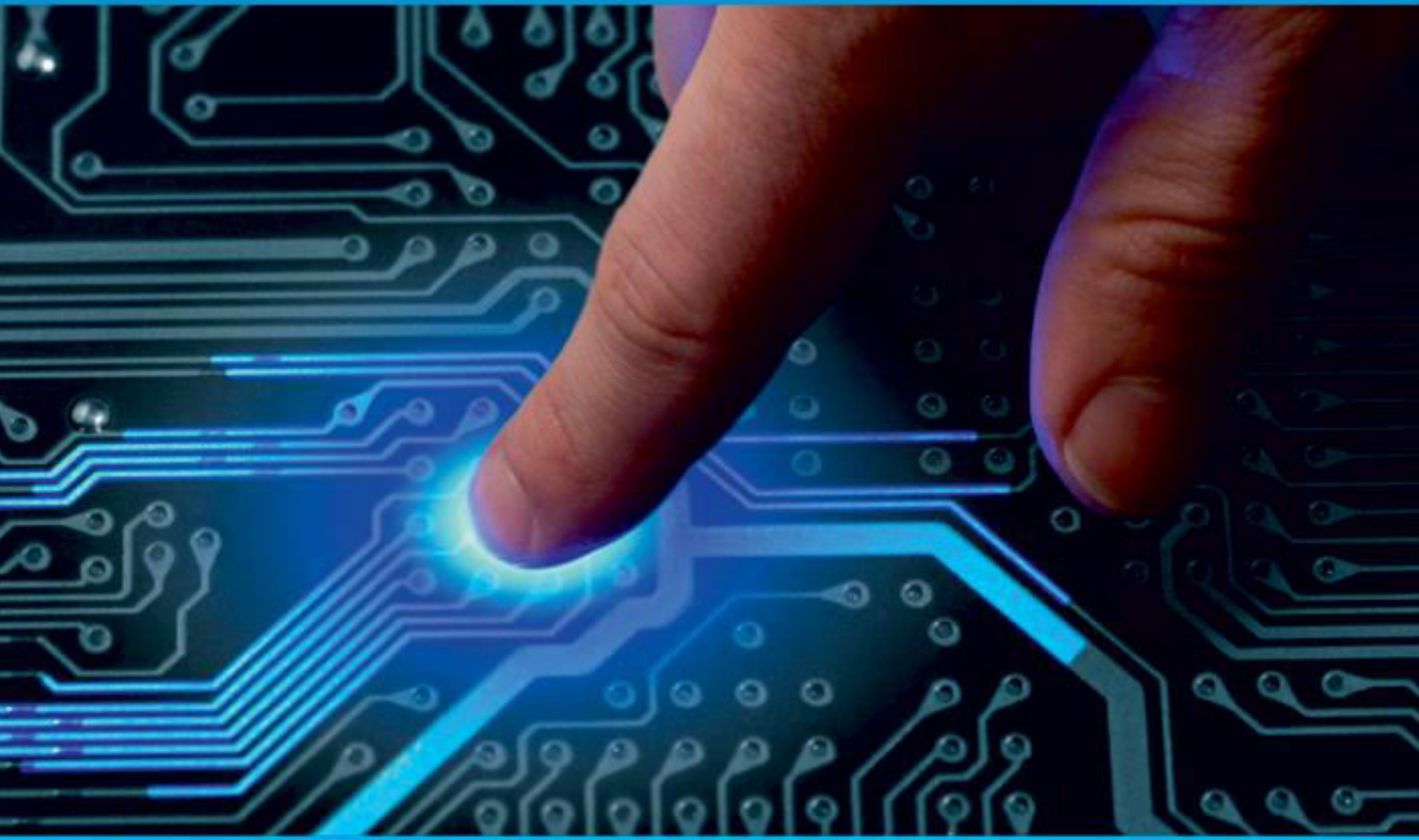
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

| DOI: 10.15680/IJIRCCE.2022.1004036 |

Design of Secured Web Application for E-Voting

Mr.P.Saravanabhava

Assistant Professor, Dept. of CSE, St Annes College of Engineering and Technology, Chennai, India

ABSTRACT: The higher use of information technology seems to have enhanced the technologies of governmental department services. Electronic voting machine is the example for modernized democracy. Electronic voting machine should be combined with legal procedures. Data's acquired from Voting machine after the voting process determines who will run the country. Finding the peoples choice of leader is the main aim of Voting machine. In many of the countries voting is trouble. Some of the issues in EVM are incorrect voting during elections, experience less persons involved in election process, difficulty in accessing polling stations, and deficiency in voting equipment. The proposed new internet-based voting system solves the problem in EVM. This method prposes a small learning curve, citizens will have to be trained on how to exercise their right to vote online.

KEYWORDS: voting, E-voting, electronic voting system.

I. INTRODUCTION

E-voting plays a very high role in forming a democratic society. The existing voting technique makes voters to vote by visiting their polling stations. Polling stations are installed in some public places. The proposed E-voting technology would save a lot of time for both voters and the election commission.

A Perfect Voting application should allow fully functional online voting using general household devices [1]. Vote counting can be done secretly in an automated manner. E-voting system has some issues like threats and challenges as it depends on the internet. However, it is simultaneously solving the problems faced while using current voting systems. Different sets of procedures need to be followed for the E-voting system.

To get rid of threats, different types rules related to eligibility, ballot-privacy, singular verifiability, completeness, fairness, universal verifiability, and robustness need to be established.

The proposed Voting Application is an Online voting method. In this system, citizens who are over the age of 18 and all sexes should be able to cast their ballot without visiting polling stations. There is a database managed by the Indian Electoral Commission that stores all voters' names with complete information.

In this proposed method voters can easily use their voting rights online. People must be registered first in order to vote. For security reasons the system administrator need to register everyone. System administrator registers voters on a special registration form.

Citizens those who wish to register should contact the system administrator to submit their contact details. The verification of each citizen is done using existing informations such as AADHAR, PAN-Card, Passport, etc., by the registration authority, the individual is therefore registered as a voter by the Indian Electoral Commission.

After registration process, the voter will receive a Voter_Id number and a password and using these
credentials the citizen can log in to the system and use the services of the system, e.g. Voting, reviewing results, etc. If invalid details are submitted by the user, the citizen will not be registered and he will not be able to vote.

III. ISSUES WITH EXISTING SYSTEMS

A. *Current Scenario*

In the past days, the voting was done using paper ballot. Due to advancement in technology, Electronic Voting Machines were developed and like any technology, it also has its advantages and disadvantages.

B. Election Commission of INDIA

The duties of the Election Commission of India (ECI) as established by Article 324 of the Constitution are to ensure that the election process is being performed in a fair and free manner [2].

For any election to qualify as free and fair, the standards are as follows:

i. Individuals must be meticulously verified as eligible voters;
ii. Voters must be able to vote only a single ballot, which should be anonymous and allowed to opt-in private space;
iii. The ballot box or any storage medium must be secure and carefully surveyed during the election, voters must only have the power to cast in the vote note redact them;
iv. After the election is over, the votes must be extracted from the ballot in presence of observers from all participating parties, the votes and the voters must remain anonymous;
v. When or if there is any doubt in the result the verification of votes must be available;
vi. The vote of the respective voter must go to the candidate he/she cast it to.

Over the last few centuries, the paper ballot satisfies all the six needs for a fair and free election. However, the way EVMs are being used in India for general elections dissatisfies the requirements shown above.

Election Commission of India then integrated the EVMs with the assurance of a “paper backup” or “paper trail” as is performed in different states/countries. This was an easy and practical way to meet the last two needs mentioned.

As intended, the “paper trail” procedure is supposed to support the process of voting, described below:

When the voter gets approved then he/she can make decisions in the ballot. If they confirm the choice displayed to them, the vote is being recorded in some storage medium [3].

After that the EVM prints out the choice made by the voter in the receipt form and gets deposited in the ballot box, which poll works should be watching.

“If the election is later disputed or found being rigged, officials can optically scan these paper ballots or hand-count them accordingly.”

C. Electronic Voting Machine

Electronic voting machines (EVMs) were originally developed to smoothen the process of voting. They were a great success but created new problems of their own. Furthermore, EVMs do not satisfy the basic legal requirements that were being established in the IT Act 2000 [4].

The current version of EVMs that are being used in the election process cannot verify the identity of the voter. This leads to a new problem, which if e xploited any number of fake and bogus votes can be cast in the ballot.

D. Related work

E-voting applications’ trails have been carried out by several countries, depending on their capabilities to carry out such an event. Some of the success stories are listed:

In 2000, elections were carried out using an E- voting system in the United States’ election. Even though it was only carried out in some parts of Florida, it marked its name in the history of E- voting systems’ development [5].

In 2002, an electronic voting system was tested in the United Kingdom. During this process, 16 authorities were rewarded for building that E- voting system. For the same, 18 more authorities were awarded after a year.

In the year 2004, the United States conducted the election using an E-voting system DRE for the first time in history at a national level.

The first mass internet-based voting was recorded in the French Presidential election. In the year 2007, history was made in France in E-voting which involved more than 31,000 voters to participate in the 2007 French Presidential election.

In the year 2014, 17,60,000 ballots were recorded in the election of the Ministry of National Education of France.

E. Problem with Existing Systems

- Costly and time taking: The stages of gathering and registering the data into the database take too much time and is expensive to conduct, for exa mple, time and money is spent in printing data capture forms, in preparing registration stations together with human resources,

and thereafter advertising the days set for registration process including sensitizing voters on the need for registration, as well as time spent on entering this data to the database.

- More than required paperwork: In the current process a lot of paper usage is involved which leads to other problems like storage spacing, environmental degradation, global warming, etc.
- Mistakes are made during filling information: Mistakes are part of being human; It is very unheard-of human beings being 100% efficient in data entry.
- Loss of registration forms: Registration forms are sometimes lost after being filled in with voter information, in most cases, these are difficult to follow-up. Hence, many individuals remain unregistered even though they were elig ible and willing to cast their vote/ballot.
- Inadequate time provided to verify the voter register: This seems to resurface again and again as a big pain point for voters, the ability to verify their voter records are correct gives them the peace of mind every voter should have of their vote being considered every time they vote.

III. PROPOSED ARCHITECTURE

In this paper, an e-voting application is proposed.

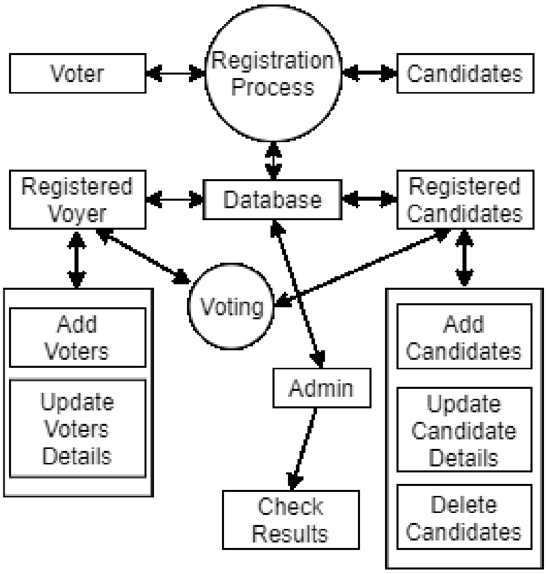


Figure 1: Application’s ER diagram

It has two main components: Voter and Admin/Election commission.
It consists of two phases: Registration phase, Login phase, and Voting phase.

A. Registration phase

1. The voting process starts with the registration of the voter.
2. If the voter is registered already, he/she can go to the login page to cast his/her vote.
3. If the voter has not been registered, He/ She needs to go to the registration center with valid documents.
4. There he/she will fill a form and submit it with photocopies of valid documents as proofs of various kinds.
5. If elig ible he /she will get his/ her voter id card after some week and will be eligible to cast a vote.

If not, the officer will contact you about the reason and how it can be solved

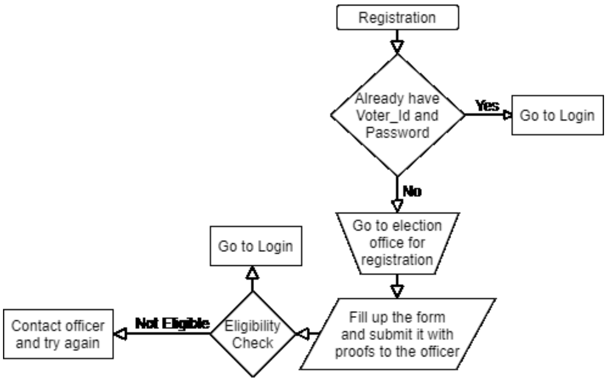

Registration
Already have Voter_Id and Password
Yes
Go to Login
No
Go to election office for registration
Fill up the form and submit it with proofs to the officer
Eligibility Check
Go to Login
Not Eligible
Contact officer and try again

Figure 2: Registration Phase

B. *Voting phase*

1. To cast a vote, open the login page.
2. Enter your voter_id and password to log in.
3. Select the candidate you want to vote for from the list.
4. Check Or verify your vote.
5. Submit, to end your voting process.

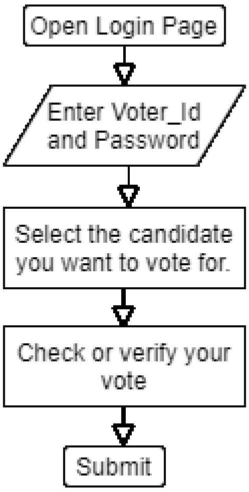

Open Login Page
Enter Voter_Id and Password
Select the candidate you want to vote for.
Check or verify your vote
Submit

Figure 3: Voting Phase

IV. LEGAL ISSUES

Any application in these times has to follow some legal rules and must be under some regulations of some sort.

A. *Remote voting:*

Remote elections at the moment fail to provide any kind of super visional factor. When the individual casts its votes in the voting booth, they are given some privacy or space, but still kept in surveillance from a distance; which is not possible in the E-voting system. While an individual is casting votes in the election process, a family member or coercer can watch over your shoulder and compromise the process [6]. The website on which the application is hosted can be compromised by an attacker/ hacker.

B. *Transparency:*

In today's election scheme, an individual has no way to verify that his/her vote is counted correctly and fairly [7]. For any reason, if an individual's vote gets misplaced, there is no way of even realizing that the vote is lost.

Transparency in the electoral process is very tricky and difficult to achieve. Sometimes it can be dangerous as it may leak more information than it should or is allowed to.

C. Voter privacy:

In an election process, voter's privacy or anonymity is the key element. It is forbidden by law to even know what another individual opted for in the ballot. To achieve, the privacy of each voter, no vote should be traceable back to the voter [8].

V. SECURITY ANALYSIS

No web application is entirely secure in this world; bad people (attackers) catch up with developers and all very quickly [9]. Va rious threats can harm the E-voting system in different phases of security leaving an unsecured system.

A. Denial of Service

Denial of Service (DOS) is an attack which intends to or successfully shut down a network or a system, which makes it inaccessible to the authorized users. This attack can disrupt the election process, even take down the whole network

B. Viruses

Viruses are a malicious piece of code that attaches itself to a host intended to spread from one to another. It can replicate itself and even copy it to other programs. The infected vulnerable system may lose data, admin control, sensitive data, and who knows what. if an E-voting application gets infected then it may compromise the election or perform several malicious tasks.

C. Worms

A worm is a malicious program that replicates itself and spreads to the network or any other connection present without any human interaction. It doesn't need to attach itself to any software program i.e. it does not require any host to carry the code. Worms can harm E-voting application by either compromising server storage or network bandwidth. If programmed accordingly, the ability to overwrite file and change result of the election, bringing the purity of the ballet into danger.

D. Trojan Horses

A trojan horse is a program or file that appears to be safe but may be performing tasks like giving admin access to the system or network, sending information to an attacker(s), and so on. They are an immense reason for concern to the confidentiality and integrity of the E-voting application(s) and/or systems' network. The data of the voting process or voters can be stolen.

E. Physical Attacks

There are several ways in which an E-voting system can be compromised physically. They may damage, disrupt, change, or destroy computer equipment or the data itself. Physical attacks on E- voting can be a scheme of a candidate/party to sabotage the election process. It may also be an attempt to steal the voters' personal information for illegal uses. So, the infrastructure of the E- voting system should be kept secret.

VI. NULLIFIERS OF THREATS AGAINST E-VOTING SYSTEMS

To nullify different types of threats, some mitigation controls are suggested. They don't ensure absolute safety but act as safeguards to the network or system, making them difficult to compromise.

A. Authentications Schemes

Logical and physical access to the E-voting system(s) should be allotted based on credentials and rights on the basis or either role -based policy or need to know basis. Administrators and voters should gain access with the help of non-trivial authorization and authentication mechanis ms for improved security[10]. For example, Public Key Infrastructure was applied in the Estonian E- voting System (EstEVS), which enabled voters to vote only when they used their authentication and Digital signature certificates.

However, t raditional methods with some tweaks can also provide great authentication method like making it mandatory for the user to set complex credentials.

B. *Phishing Scams*

A Social phishing scam could be avoided by spreading knowledge of E-voting application about different tactics using which phishing scam could be launched [11].
The above can be done only if the educators are up to date with the newest methods of e xploitation. Technical phishing scams could be more harmful than the social phishing scams as they have the ability to disrupt the election process.

C. *Mutual authentication*

This is the method in which the client is required to authenticate the server and server must authenticate the client for further interaction.

D. *Integrity Threats*

Integrity threats are those which makes you question the integrity of the data. Integrity threats in an E-voting application can be minimized by forbidding changes during the active stages of the voting process [12]. E-voting application must be reviewed by an independent third party before deployment to verify that it does exact ly what it is supposed to and further to find any kind of anomaly in the code. Using Cryptographic techniques while data transmission can reduce integrity threats.

E. *Subverting System Accountability Solutions*

The usage of checksums and encryption on the audit trails helps to catch or to prevent any kind of changes to the file system. It helps to reduce the risk of running source code with side effects.

F. *Network Infrastructure Through Redundancy*

Honey pots and Cryptograph can be used to minimize attacks on the network or the system. However, preventing DOS attack can be quite challenging some times.

G. *Open Source Systems in E-Voting*

The idea of including open source systems in E- voting has been suggested. It’s still not a wise decision to include an open-source system running E-voting over the internet. An open-source system cannot be trusted more than a closed source system. In an art icle by Ken Thompson entitled “Reflections on Trusting Trust” it was stated that “you can’t trust code that you did not totally create yourself” [13]. Any application written in a way that it is derived from an ingenious piece of code can be used to include or insert backdoors in the application.

VII. RESULT ANALYSIS

Ideal Electronic voting or any voting method for that matter should follow certain parameters for the successful voting process[14].
In order to perform an internet-based election, some parameters need to be addressed.

A. *Ballot privacy*

No one other than the voter themselves cannot acquire knowledge of someone’s ballot.

B. *Individual verifiability.*

The voter must have an option to verify or confirm after the voting process.

C. *Eligibility*

Only the legal voter would be allowed to enrol in the voting process.

D. *Completeness*

Each and every vote should be counted precisely.

E. *Uniqueness*

Every voter should only be allowed to vote once during an election. An individual should not be allowed to vote again.

F. *Robustness*

No one should have the ability to modify the results during the process of counting and/or tallying.

G. *Coercion-Resistance*

The voter should not be able to prove who he/she casted their vote to.

H. *Fairness*

Anything or anyone should not possess the power or ability to influence the result of the election.

I. *Receipt-freeness*

No need for creating any sort of paper receipt or acknowledgment during or after the voting process

VIII. CONCLUSION

Proposed internet-based voting system manages the voter's information, which makes the voting process easier, citizens can just simply login and exercise their right to vote. This online voting system is for conducting the elections in a free and fair manner hence tries to include all the advantages of existing voting solutions. This method manages the heavy and repetitive task of vote management by counting the number of votes received by individual candidates and later the number of votes received by each political party. The Election Commission of India independently owns and maintains the voter and election databases with the complete information. This database is stored in a safe location and only higher officials of the Election Commission of India have the access.

This online system allows all eligible citizens to register themselves on the system. After which they can log in by their password and vote. This system does not allow any person to vote more than once.

All the votes are recorded and will be stored on the databases. The result is counted in a few minutes through the pre-written program, which keeps tallying the results in real-time. This method removes all the difficulties in traditional methods of voting, cost and time. The user-friendly design makes it easy to use and troubleshoot.

REFERENCES

1. Yifan Wu, An E-voting Systembased on Blockchain and Ring Signature,: University of Birmingham, 2017.
2. The problem with EVMs by Subramanian Swamy, https://www.thehindu.com/opinion/op-ed/The-problem- with-EVMs/article13369610.ece, 2 september 2010.
3. Orhan Cetinkaya, and Deniz Cetinkaya, Verification and Validation Issues in Electronic Voting, :Institute of Applied Mathematics, METU, Ankara, Turkey. 2014.
4. L. Christian Schaupp, Lemuria Carter, E-voting: from apathy to adoption: Journal of Enterprise Information Management, 2005 .
5. e-Envoy, in the service of democracy; a consultation paper on policy for electronic democracy. In. London: office of the e-Envoy, Cabinet Office, 2002.
6. Electoral Commission, Modernising elections: A strategic evaluation of the 2002 electoral pilot schemes. London: The Electoral Commission, 2002..
7. M.L. Markus and D. Robey, Information technology and organization change: causal structure in theory and research, Management Science 4(5) (1988).
8. Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Brief aan de Tweede Kamer over heroverweging Kiezen op Afstand (Letter to the Parliament regarding the reconsideration with respect to e-voting). In. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 2002.
9. Olsson and J. Åstrom, eSweden: Hare or Tortoise? In Internet Voting. Present states and future perspectives IPSA Research Committee 05. Marburg, 2002.
10. W.J. Or likowski and D. Robey, Information technology and the structuring of organizations, Information Systems Research 2(2) (1991), 143–163.
11. Pratchett, The implementation of electronic voting in the UK, London: Local Government Association, 2002.
12. S. Bundesrat, Bericht ¨uber den Vote ´electronique; Chancen, Risiken und Machbarkeit elektronischer Aus¨ubung politischer Rechte. In: Schweizerischen Bundesrat, 2002.
13. F.I. Solop, Digital Democracy Comes of Age in Arizona: Participation and Politics in the First Binding Internet Election. In American Political Science Association National Conference. Washington DC, 2000.
14. B.Watt, Implementing electronic voting: A report addressing the legal issues raised by the implementation of electronic voting. In: University of Essex, 2002.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details