IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 56-59

A Study on Technological Development in Indian Voting System from Document-Based Ballot System to Biometric System

K.Kanimozhi[1], Dr.K.Thangadurai[2]
Research Scholar, PG and Research Department of Computer Science, Government Arts College, Karur, Tamil Nadu, India
Head and Assistant professor, PG and Research Department of Computer Science, Government Arts College, Karur, Tamil Nadu, India

Abstract: *It has always been an arduous task for the election commission to conduct free and fair polls in our country, the largest democracy in the world. Rupees have been spent in crores on this to make sure that the elections are riot free. But, now- a -days it has become common for some forces to indulge in rigging which may eventually lead to a result contrary to the actual verdict given by the people. In this paper, it has been made a study on different voting technologies that had been incorporated for earlier elections and the future technology that will be made for high secured voting system; it is none other than biometric voting system.*
Keywords: *Voting system, Types, Electronic voting, biometric based voting.*

I. Introduction

It has been demonstrated that as voting systems become more complex and include software, different methods of election fraud become possible. Others also challenge the use of electronic voting from a theoretical point of view, arguing that humans are not equipped for verifying operations occurring within an electronic machine and that because people cannot verify these operations, the operations cannot be trusted (Bar-El, 2015). Furthermore, some computing experts have argued for the broader notion that people cannot trust any programming they did not author (Thompson, August 1984). Critics of electronic voting, including security analyst Bruce Schneier, note that "computer security experts are unanimous on what to do (some voting experts disagree, but it is the computer security experts who need to be listened to; the problems here are with the computer, not with the fact that the computer is being used in a voting application)... DRE machines must have a voter-verifiable paper audit trails... Software used on DRE machines must be open to public scrutiny" (Schneier, 2008) to ensure the accuracy of the voting system. Verifiable ballots are necessary because computers can and do malfunction, and because voting machines can be compromised.

There was a large transition in voting technology from the first election till now. Thus, it is important to study those prior technologies before developing the biometric based latest approach.

II. Technological Developement

Present technology used for election is e-voting machine. Before that so many machines are tried but the result was not worthy .Let us see those ancient machine models in detail.

a. Paper-based electronic voting System
b. Direct – recording electronic (DRE) voting
c. Public network DRE voting system
d. Online voting
e. Electronic ballots

a. Paper-based electronic voting System

Sometimes called as "document ballot voting system", paper-based voting systems originated as a system where votes are cast and counted by hand, using paper ballots. With the advent of electronic tabulation came systems where paper cards or sheets could be marked by hand, but counted electronically. These systems included punched card voting, mark sense and later digital pen voting systems.

b. Direct – recording electronic (DRE) voting system

Direct-Recording Electronic (DRE) Voting Machine: A voting machine that is designed to allow a direct vote on the machine by the manual touch of a screen, monitor, wheel, or other device. A DRE records the individual votes and vote totals directly into computer memory and does not use a paper ballot.

c. Public network DRE voting system

Public network DRE voting system. A public network DRE voting system is an election system that uses electronic ballots and transmits vote data from the polling place to another location over a public network. ... This includes Internet voting as well as telephone voting.

d. Online voting System

An alternative voting channel to increase voter participation, reduce election costs while upholding the highest security, verifiability and integrity standards. Online Voting enables voters to cast their vote privately and easily from any location and on any device with Internet access (PC, tablet, Smartphone, etc.), ensuring maximum election engagement by enabling remote and disabled voters to participate on equal terms. Voter privacy, election integrity, end-to-end security, vote correctness and full verifiability (individual and universal) are guaranteed via advanced cryptographic protocols. This enables election officials to assure citizens that their votes remain cast-as-intended, recorded-as-cast and counted-as-recorded.

In addition to the added accessibility and security, operational efficiencies result from significantly reduced costs and the delivery of more timely and accurate results. To better cater the needs of private sector organizations, Scytl has developed Invote, a secure online voting solution for membership organizations and associations. Invote simplifies the whole election process and enables voter participation from anywhere and on any device through a transparent and convenient way of voting.

e. Electronic ballots or E-Voting System

Electronic voting systems may use electronic ballot to store votes in computer memory. Systems which use them exclusively are called DRE voting systems. When electronic ballots are used there is no risk of exhausting the supply of ballots. Electronic voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting votes.

Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results.

Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

In general, two main types of e-voting can be identified:

- e-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations);
- Remote e-voting via the Internet (also called i-voting) where the voter submits their votes electronically to the election authorities, from any location.

Drawbacks of Electronic Voting System:

- With recent elections in the United States, many software programmers have claimed that the electronic voting machines are vulnerable to malicious programming and if it gets affected then any hacker can hack the machine and can tamper the vote counts easily.
- Many physically challenged people have complained that the touch base screen is not efficient enough to capture the vote accurately. Sometimes it leads to the voter ending up voting for someone else unintentionally.
- Although it takes the time to count votes that were captured using paper ballot but people fully trust the process as high technology are also vulnerable to hackers attack.
- The biggest change with technology is that no matter how much data it records but a single virus can destroy the entire data storage. The electronic voting machines which were used during the elections are susceptible to damage which will result in loss of data.
- The highly humid area and those areas which receive frequent rainfall are not suitable for casting votes using electronic voting machines. As machines are prone to damage due to high humidity level thus usage of electronic voting machines are not advisable in such areas.
- Most of the electronic voting machines used in the country were foreign manufactured, which means the secret codes that control the electronic voting machines are in foreign hands and they can be used to influence the election results.

- Fake display units could be installed in the electronic voting machines which would show manipulated numbers but originally fake votes could be generated from the back end. This process does not need any hacker to hack the software. Such fake display units are easily available in the market.
- Most of the electronic voting machines used in the country do not have any mechanism by which the voter can verify their identity before casting the vote due to which fake voters can cast numerous fake votes.
- The electronic voting machines also do not generate a slip confirm the candidate one voted post pressing the button. In these cases, it is very easy for a criminal or a hacker to manipulate the votes. If the machines would generate such slips, then people could verify if the number of votes captured via EVMs was in line with the details on slips received by the voter.
- Electronic voting machines can be tampered during its manufacturing and in such cases, it does not even require any hacker or malware to manipulate the actual voting.

III. Methodology Of Biometric Voting System

Biometrics is a method of identify a person based on physical or behavioral characteristics. Examples of biometric information used to identify people include fingerprint, voice, face, iris, handwriting, and hand geometry. Biometric sample is compared sequentially to a set of stored samples to determine the closest match. .

The verification method provides the best combination of speed and security. Unprecedented growth in electronic transactions has underlined the need for a faster, more secure and more convenient method of user verification than passwords can provide.

Biometric identifiers offer several advantages over traditional and current methods. Passwords can be forgotten, shared, hacked or unintentionally observed by a third party. By eliminating these potential trouble spots, only biometric technology can provide the security, with convenience needed for today's complex electronic landscape.

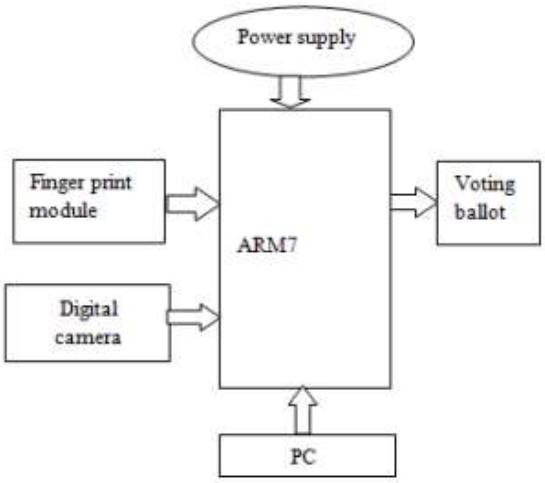

Figure1: Block diagram of Biometric voting system

a. Algorithm Of Biometric System:

Step1: First initialization of process.
Step2: For identification the voters data and their fingerprint ,face and voter details are stored in personal computer. It means registration of voter.
Step3: Check if the voter is valid or not by using their stored data. That is captured finger and face is compared with stored data in personal computer.
Step4: If the voter is not able to give their vote or not registered then message is display the person is invalid on LCD.
Step5: If voter is valid, then go to next step.
Step6: Check if the voter has already voted or not.
Step7: If he has already given his vote, then message is displayed that he has already voted and is prevented from voting for the second time.
Step8: Else, if the candidate is voting for the first time, then he is allowed to vote.
Step9: Voter can denote their vote. ‘
Step10: Result is stored on PC and display the result on LCD display after completion of complete voting.

IV. ADVANTAGES OF BIOMETRIC VOTING SYSTEM

- Increase security – Provide a convenient and low-cost additional tier of security.
- Reduce vote fraud by employing hard-to-forge technologies and materials, such as minimize the opportunity for identification fraud and buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For example, prevent unauthorized use of lost, stolen or "borrowed" ID cards.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.
- Make it possible, automatically, to know who did what, where and when. But the technicality can make it difficult for the voter in other country to realize that he/ she might not have voted. So celebrating biometric voting is still premature.

V. CONCLUSION

Thus the advent of this biometric voting system would enable hosting of fair elections in India. This will preclude the illegal practices like rigging. The citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy.

REFERENCES

[1]. Bar-El, H. (2015). Why secure e-voting is so hard to get.
[2]. Schneier, B. (2008). *Wayback Machine What's wrong with electronic voting machines?*
[3]. Thompson, K. (August 1984). Reflections on Trusting Trust.
[4]. International Journal of Engineering Research –Offline and online E-voting system with embedded security for real time application ,Alaguvel. R, Gnanavel .g.
[5]. RFID based biometric voting machine linked to Aadhaar for safe and secure voting Madan Mohon Reddy,D.Srihari International Journal of science, Engineering and Technology Research (IJSETR).
[6]. IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. II (Jan - Feb. 2015), PP 57-65www.iosrjournals.org Biometric System Based Electronic Voting Machine Using Arm9 controller 1M.Sudhakar, 2B.Divya Soundarya Sai,1Professor in ECE, 2II Year M.Tech,Dept of ECE,CMR College of Engineering &Technology,Hyderabad, TS-India.
[7]. Biometric Voting machine (BVM) using IOT .By K Dinesh, G Sai Nadha , B .Tech - ECE (2nd year) ,RGUKT- RK Valley .The election procedure dates back to ballot papers. Ballot papers had been used for almost 5-6 decades. With the advent of technology, ballot papers have been replaced by EVM (Electronic Voting Machine).
[8]. www.efymag.com
[9]. www.utdallas.edu
[10]. www.m2sys.com