International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-12, Mar 2018

# Analysis & Survey Paper on Voting Systems & Technologies around World

[1]Vaibhav Thakare, [2]Dr. Ayesha Butalia, [3]Swapnil Randhave, [4]Sushant Nanaware, [5]Sagar Bhor
[1,2,3,4,5]Department of Computer Engineering PGMCOE, Wagholi, Pune University, Maharashtra, India.
[1]vaibhav.vat@gmail.com, [2]ayeshabutalia@yahoo.co.in, [3]swpnlrandhave@gmail.com, [4]sushant2328@gmail.com, [5]Sagarbhor70@gmail.com

**Abstract – There are many of voting systems used widely in almost all countries. This voting system is very important aspect to elect organization or government. Description of this system is important for analyze the flexibility of system and to study the loopholes of different types of current voting systems. Analysis will help to improve the voting systems. To study the current voting systems analysis should be done. According respective countries and there population they have accepted respected voting system. Every system has register a fault or bogus voting cases due its working methods to emphasis the development of more secure automated and flexible systems.**

***Keywords—EVM, Voting, Voting system in different countries, Online voting***

## I. INTRODUCTION

Our earth is divided into fragments; we call them countries where group of people lives and handle their respective areas, functioning, development, import export and many other important works. To make this possible organization is needed. This organization manages administrations. To build this organization, citizen of that country use vote system which emphasis on citizen mandate choice. These voting systems have been evolving through decades. Origin


late Middle English: from Latin *votum* ‘a vow, wish’, from *vovere* ‘to vow’. The verb dates from the mid 16th century. Different countries use different voting systems. Some countries elect government and others elect organization to govern themselves using voting system. But there are flaws in all most all voting systems. People have been witnessing this fault since past long time or since its origin.

### *A. Brazil*

In Brazil, the largest nation in South America, currently, all votes are cast by electronic voting machines. The Brazilian Supreme Electoral Court authorized the use of Electronic voting technology in the 1996 Brazilian municipal elections. In 2000, the Brazilian government had converted to fully electronic voting and deployed over 400,000 kiosk-style machines in elections that year. Voters in Brazil use an electronic voting device that, for each office, displays the choices and prompts the voter for his or her vote. The voting machines feature an integrated screen and keyboard .To vote for a candidate, voters only need to press on the keyboard the number designated for a particular candidate. The candidate’s picture then appears on the screen. Voters can confirm, reject, choose another candidate or start the selection process again. The Brazilian electronic voting technology is unusual in that the voting machine itself tallies the votes once voting finishes, producing both digital and printed reports of the number of votes given to each candidate. 12,000 machines used to produce a paper ballot that the voter could peruse and deposit in a box for recount. These paper-trail machines were successfully used during the election [2].

### B. Spain

Spain has experimented with various forms of electronic voting. In the March 14, 2004 general elections, numerous small-scale, non-legally binding electronic voting trials were successfully conducted. These included diverse technologies in addition to strictly Irish-style electronic voting systems, such as Internet and SMS remote voting. On November 16, 2003, three e-voting pilot tests were successfully conducted during the elections to the Parliament of Catalonia. This included remote voting via the Internet for eligible voters living abroad, and touch-screen voting coupled with an electronic counting system (developed by Demotek) [11].

### *C. Belgium*

In Belgium Electronic voting was approved by law in 1994, and widely used in the 1999 and 2000 general and municipal elections. In the general elections of May 18, 2003, 3.2 million Belgian citizens were able to vote electronically. Belgium’s apply similar approach as Ireland’s in that it does not modify the voting process, but rather replaces the ballot paper with a machine at the polling station, and then uses an electronic counting system to tally the results. In 2003, an audit report released by the Federal Public Service of the Interior approved the systems after a simulation based on around 1 million votes [3]. Some difficulties were recorded during the 2003 voting (May 18) in the Belgian communes where electronic polling

booths were in use for the general elections, which renewed both federal assemblies of the country. Delays occurred in voting operations in some localities, causing some polling stations to have to remain open well after the official closure time of 3 p.m. Voters therefore had to wait for a long time to cast their vote in some areas. Most did wait, due to Belgium's compulsory voting system and fines for failing to do so, but it was reported that an estimated 10% of voters abstained from the ballot in certain areas [12].

### *D. Australia*

In Australia EVM started in a close election in 1998. The Australian Capital Territory (ACT) is one of eight states and territories in Australia. Members of the ACT Legislative Assembly are elected using a proportional representation electoral system known as the Hare-Clark system. Hare-Clark is a variant of the single transferable vote method used in Ireland. Electors vote by showing preferences for individual candidates. To be elected, candidate needs to receive a quota of votes. Each elector has a single vote, which can be transferred from candidate to candidate according to the preferences shown until all the vacancies are filled. In the ACT, the Hare-Clark system is used to elect 17 members from 3 multi-member electorates. The electorates of Brindabella and Ginninderra each elect 5 members, and the electorate of Molonglo elects 7 members. A close election in 1998 in the ACT found numerous problems in the state's hand-counting system, when two candidates were separated by only three or four votes. After recounting, officials discovered that out of 80,000 ballots, they had made about 100 mistakes. Ultimately, the ACT Electoral Commission adopted a new system known as eVACS, or Electronic Voting and Counting System. The system was created (by a company called Software Improvements) to run on Linux, which is a widely used, freely available open-source operating system [1]. The eVACS-based voting terminal consists of a PC and offers ballots in 12 languages, including Serbian and Farsi. The system includes English audio for vision-impaired and illiterate voters. The voter swipes a bar code over a reader that resets the machine for a new vote and calls up a ballot. The eVACS- based voting system find problems, such as difficult-tousle barcode readers and minor delays in displaying results on and after election night, it was well received by voters.

### *E. Italy*

Italian electronic scrutiny system involved in the large scale election in 2004. According to the Italian Government, the main advantages of an electronic scrutiny system would be easier and faster operations, more accurate vote counting, faster and secure transmission of results and an increase in overall election efficiency. The Italian government has not yet released detailed technical specifications of the planned electronic vote counting system [2]. A national ad-hoc Commission will assess the pilot, with particular reference to the efficiency of the system, and address any problems it may encounter. The Commission will then make any necessary recommendations in order to prepare the system for wider testing in future elections. [5]

### *F. Argentina*

Argentina started an electronic voting system in 2003. This system is based on machines already used in Brazil. The electronic voting machines (EVMs) resemble ATMs. At the time of voting each citizen shows identity documentation at the voting place and the registrar enters the voter's identity number at a keyboard with a display. If it appears OK on the display, the person is approved to vote and goes behind a partition where the EVM is located [7]. The screen of the EVM shows the first office that the voter will vote for all the political parties that presented candidates, each paired with a number. The voter chooses his or her favorite by punching a key with the number of the chosen party. The next screen shows the name and photo of the chosen candidate. To confirm the selection, the voter punches a green key. If the voter wants to change the selection, he or she punches a red key. Once the selection has been made, the voter pushes a white key and then the green key to confirm. The system also permits voters to cast "blank" votes, which in Argentina are counted in order to calculate the percentage of votes obtained by each party. After completing a vote for a particular office, another screen appears with the following office to choose and continues until the ballot is completed. At this point the EVM disables, preventing a second vote [8].

In 2006, Italy used Nedap Voting machines in the national elections. The pilot project involved 3000 electors and four polling stations. However, after the pilot project was completed, the country chose to go back to paper as it is easy to manage and cheaper.

While these countries have banned or refrained from using EVMs, there are others who have taken a systematic approach and backed the use of EVMs with paper ballots. In various parts of the United States of America as well as in Venezuela EVMs are used on a large scale but are backed by paper trails of the votes. This simple step helps the government to regularize and check the authenticity of votes and avoid any discrepancies.

### *G. United Kingdom*

United Kingdom started EVM in May 2002, tested various technological improvements to voting or vote counting, such as touch-screen voting machines while others tested techniques for voting remotely. Some Jurisdictions allowed voters to cast their ballots using electronic methods, such as interactive voice response (IVR) technology, PC-based systems and handheld mobile devices via short message service (SMS). Some of these jurisdictions allowed voters to cast ballots from PCs or kiosks in public places such as shopping centers. In the Electoral Commission's report to reviewing the e-voting trials, it found that the hardware and software performed successfully and without any significant problems. It also identified no evidence of fraud during the pilots, although it did express concerns about potential security and privacy violations [5, 6, 7, 9].England has had various pilots for the electronic voting system thereafter. However, these pilots have never led to the use of EVMs in

the country. England is one of the few countries for whom it became hard to follow modern methods in political elections, and the government plans to continue on the same path. In January 2016, the UK Parliament revealed that it has no plans to introduce electronic voting for statutory elections, either using electronic voting in polling booths or remotely via the internet

### *H. Success of Estonia*

Germany could have looked at Estonia, a small country with a population of merely 1300000. Estonia became the first country in the world to enact a law making electronic voting using the internet mandatory. It passed the law in 2005. Estonia claims to have conducted the first internet-based national election in 2007. It went for three days.

### *I. Panama*

In Panama, the first experiment with electronic voting in 15th November 1992. The system consisted of a mechanical element in which electors used bulb type switches to vote, and then pull a lever to record their vote via perforations in a paper. The experiment involved six voting machines in the metropolitan area of Panama City and San Miguelito, in the districts of Bella Vista, Parque Lefevre, Juan Díaz, San Francisco, Bethania and Belisario Porras. In 1999 elections, an electronic voting system was tested at several points in the Republic of Panama, though in the end it was not used due to a lack of consensus between political parties as to its use [11].

### *J. India*

In India first election using electronic voting is scheduled to hold from April 20 to May 10, 2004. India is the world's largest democracy with a population of more than 1 billion; India has an electorate of more than 668 million and covers 543 parliamentary constituencies, and will require more than one million electronic voting machines (EVMs). The legal approval in 1989 to allow the use of EVMs, they have been used in many state elections but never used an entire general election. Electronic Voting Machines prepared by Electronics Corp of India and Bharat Electronics. The EVM comprises two units, one for control by the polling staff and the other for the use of voters. The balloting unit requires voters to press the button next to the candidate's name and symbol and the control unit records the vote. A light next to the button glows, and a short beep sound follows indicating the vote has been cast. The polling officer then presses a switch to clear the machine for the next voter. The EVM comes in a reusable carry pack, and can operate on a battery power source in remote areas. According to Election Commission officials, each EVM can record five votes in minutes or nearly 3,000 votes in a polling day [4, 10].

### *K. Ireland*

Ireland spent millions of dollars on the installation of EVMs and to use them during the political elections. However, after spending more than 51 million pounds for three years, Ireland went forwards and scrapped the electronic voting system citing it to lack of trust and transparency in the voting machine.

### L. CURIOUS CASE OF GERMANY

Germany is the largest democracy in Europe. It introduced electronic voting in 2005. Germany imported voting machines to conduct its elections from a private company in the Netherlands. The machines were later reported to have several layers of deficiencies. Germany intended to do away with those infirmities in its machines but before that the matter reached its highest court. In 2009, the Federal Constitutional Court of Germany held that the use of electronic voting machines in elections was unconstitutional and observed that such a practice lacked transparency. Germany, unlike India, has not passed a law authorizing use of electronic voting machines for casting votes in elections.

### M. Internet Voting

While Internet voting has been utilized for national-level elections in only a few countries, it is a voting mechanism that is increasingly being explored as a means to allow access to the election process for voters who may otherwise find it difficult to go to their polling location on Election Day. Internet voting, however, presents a number of technological challenges focused on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement in and observation of the process. All of these must be comprehensively addressed for election authorities to consider moving forward with Internet voting.

The primary utilization of Internet voting in favor of a coupling political decision occurred in the US in 2000, with more nations accordingly starting to lead trials of and additionally utilize Internet voting. A sum of 14 nations has now utilized remote Internet voting in favor of restricting political races or choice. Inside the gathering of Internet voting framework clients, four center nations have been utilizing Internet voting throughout a few decisions/submission: Canada, Estonia, France and Switzerland. Estonia is the main nation to offer Internet voting to the whole electorate. The staying ten nations have either quite recently embraced it, are right now guiding Internet voting, have steered it and not sought after its further utilize, or have ceased its utilization. Cases of Internet voting in different nations around the globe fluctuate broadly in degree and usefulness. The early instances of Internet voting were less actually progressed than those being created all the more as of late. A significant number of the progressions found in Internet voting frameworks have been gone for enhancing the nature of decisions conveyed by these frameworks and meeting rising norms for electronic voting. Any reasonable person would agree that Internet voting isn't a usually utilized methods for voting. Of the 14 nations that have so far utilized it in any shape, just ten right now have communicated any expectation of utilizing it later on. In any case, Internet voting is a moderately new voting innovation and has been growing fundamentally finished the past ten years. Web voting appears to fit, for some nations, a

specialty corner of the appointive procedure. It is to a great extent focused at the individuals who can't go to their surveying station face to face on Election Day. Truth be told numerous more nations have communicated or demonstrated an enthusiasm for the utilization of Internet voting, particularly when they have huge quantities of ostracize voters. Nonetheless, the execution of Internet voting, as indicated by rising norms, is an exceptionally specialized exercise. It can likewise offer some troublesome political conversation starters if the point is to encourage the incorporation of substantial quantities of exile residents in the political procedure. The details of executing Internet voting frameworks are generally a consequence of endeavors to accommodate the utilization of Internet voting with rising and existing guidelines to which races and electronic decisions ought to follow. These guidelines incorporate the requirement for secure online voter confirmation, assurance of the mystery of the vote, suitable straightforwardness systems, testing and accreditation administrations. The requirement for secure online voter verification instruments might be one of the greatest obstacles in actualizing Internet voting. It exhibits a test for some settled popular governments, which frequently don't have ID card frameworks with secure online validation systems. In assessing the utilization of Internet voting since 2000, various imperative subjects develop:

Trust in Internet Voting – as of now examined, confide in the appointive procedure is fundamental for fruitful vote based system. In any case, trust is an intricate idea, which requires that people settle on levelheaded choices in view of the realities to acknowledge the trustworthiness of Internet voting. The issue is that Internet voting is complex to the point that couple of voters has the specialized aptitude important to settle on the educated choice to put their trust in it. To adjust for the innate many-sided quality of Internet voting, additional measures should be taken to guarantee that voters have a sound premise on which to give their trust to Internet voting frameworks. Specialized foundations and specialists can assume a vital part in this procedure, with voters believing the procedural pretended by autonomous organizations and specialists in guaranteeing the general trustworthiness of the framework, instead of their own constrained comprehension of how Internet voting functions and the confirmation systems utilized.

Various components can be utilized to empower the advancement and upkeep of trust in Internet voting frameworks. One of the basic approaches to empower trust is to guarantee that data about the Internet voting framework is made freely accessible. The framework should likewise be dependable, and measures to guarantee the respectability of the framework are essential. An imperative part of honesty is guaranteed through testing, accreditation and review components. These components should show that the security concerns introduced by Internet voting have been enough managed, and should perceive that there are a few parts of security that are outside of the control of the Internet voting framework –, for example, the gadgets (i.e., the PCs) that voters use to cast their tallies.

Because of the characteristic absence of straightforwardness with Internet voting, it is critical to isolate the obligations regarding distinctive phases of the Internet voting process. Such a partition of obligations will make it harder to control the framework. Permitting the rehashed throwing of Internet votes, with just the last vote being tallied additionally creates trust among voters. Making the Internet voting framework irrefutable, with the goal that the outcomes can be autonomously confirmed against the votes cast, is an undeniably imperative put stock in component, in spite of the fact that this should be done in a way that does not disregard the mystery of the poll. At last, Internet voting frameworks ought to be subjected to different assessment components.

The Secrecy and Freedom of the Vote – Ensuring the mystery of the vote is a critical worry in each voting circumstance. On account of Internet voting from unsupervised situations, this guideline may effortlessly turn into the primary test. Given that an Internet voting framework can't guarantee that voters are throwing their tallies alone, the legitimacy of Internet voting must be exhibited on different grounds. One important contention is the comparability of Internet voting with postal voting; a strategy for voting considered gathering models of mystery by the Venice Commission. The opportunity to rehash and wipe out an Internet vote is a typical contention for the acknowledgment of Internet voting, as it implies that a vote purchaser or coercer won't know for beyond any doubt which ticket will be meant a voter. At last, Estonia has contended that the rule of mystery involves a commitment to give the chance to a mystery vote, however that voters are allowed to pick less mystery voting alternatives on the off chance that they want.

Availability of Internet Voting – Improving openness to the voting procedure is regularly referred to as a purpose behind presenting Internet voting. The availability of voting frameworks, firmly connected to ease of use, is a global standard for races, and is important not just for voters with inabilities and etymological minorities, yet additionally for the normal voter. Web voting can significantly affect the availability of the voting procedure. It is critical that voters, particularly the individuals who may have extraordinary availability issues, are engaged with the improvement of any Internet voting framework. The manner by which voters are recognized and validated can significantly affect the ease of use of the framework, yet an adjust should be found amongst availability and trustworthiness.

The voting procedure itself, and vote-confirmation instruments, can likewise be hard to plan in ways that are available to all. Voters will frequently request that Internet voting be made accessible through the finish of typical voting, yet the term of voting should be resolved while considering different variables, for example, any prerequisites for Internet voters to have the capacity to cast a paper poll. The expansion of PC working frameworks and web programs presents

Internet voting framework engineers with expanding challenges in making their frameworks practical on all or a large portion of these working frameworks and programs.

A counterargument can be made identified with the "advanced gap" as far as the openness of Internet voting. Distinctive gatherings in the public eye have diverse levels of access to the Internet. Subsequently, the arrangement of Internet voting in social orders where there is extremely unequal access to the Internet will differently affect availability for different groups. Obviously, these groups may have altogether different voting inclinations, which could have suggestions for the aftereffects of the decision.

Indeed, even in all around created majority rules systems, more princely voters might have the capacity to vote from the solace of their own homes, while others may need to require significant investment off work to hold up in line to vote. The conceivable unequal effect on availability made by the arrangement of Internet voting would be much more extreme if Internet voting were the main methods for throwing a vote. Be that as it may, as can be seen even where customary voting systems are likewise set up, Internet voting can make openness concerns, despite the fact that the availability of these other voting instruments could be enhanced keeping in mind the end goal to adjust.

Constituent Stakeholders and Their Roles are: The presentation of Internet voting essentially changes the part that partners play in the appointive procedure. Not exclusively do new partners, for example, voting innovation providers, expect conspicuousness in the Internet voting process, however existing partners must adjust their parts so as to satisfy their current capacities. While electronic voting as a rule requires changes in the parts of these partners, the presentation of Internet voting, specifically, changes the parts in a significantly more key way as the demonstration of voting is taken outside of the surveying station.

This new system of partner parts and connections might be hard to oversee well, and a portion of the different partner requests might be opposing (for instance, they may take diverse positions on the divulgence of data on the Internet voting framework). Fundamental to this new system of partner connections is open organization, particularly the part of the EMB. Open organization and the EMB will set up the lawful and administrative structure for the usage of Internet voting; and this system will characterize the parts and privileges of the different partners in the Internet voting process. The EMB will likewise need to deal with the execution of the Internet voting innovation, guarantee control is kept up finished the provider and encourage the open contribution of every single applicable partner amid usage. An open data strategy will be basic to the EMB's communications with partners to create trusted relations while actualizing Internet voting.

Web voting presents evident difficulties for party survey watchers and eyewitnesses. While the part of onlookers in the per-race period will be like their part with different types of electronic voting as talked about above (e.g., legitimate structure, outline prerequisites, testing and affirmation, security, and so on.), spectators will be not able make a precise appraisal of the voting and tallying process. Eyewitness gatherings and political gatherings should consequently outline perception procedures on account of this and must be real to life with general society about any confinements of their evaluations. In the meantime, Internet voting presents a few new components and purposes of request for decision onlookers. These incorporate assessing the security of voting servers, evaluating the EMB's observing of voting server security and danger reaction designs, and the working of Internet Service Providers (ISPs)44. Similarly as with different types of electronic voting, IT ability will be basic to such endeavors. Eyewitnesses may likewise utilize overview methods to check voters' involvement with Internet voting, including their level of trust in the framework.

EMBs should be touchy and receptive to restriction and worry about the presentation and utilization of Internet voting frameworks. There will probably dependably be some restriction to such frameworks; be that as it may, to overlook resistance and concern is exceptionally hazardous. Indeed, even little gatherings contradicting voting innovation can have a huge effect by raising worries that resound with the general population. EMBs that neglect to react to worries about Internet voting may lose control of any open civil argument in a way that could be lethal for usage. Proactive engagement with adversaries of Internet voting by the EMB and endeavors to alleviate these worries will serve to diffuse conceivably harming open level headed discussions on Internet voting. It will likewise help guarantee that Internet voting does not turn into a disruptive issue in a nation's political talk.

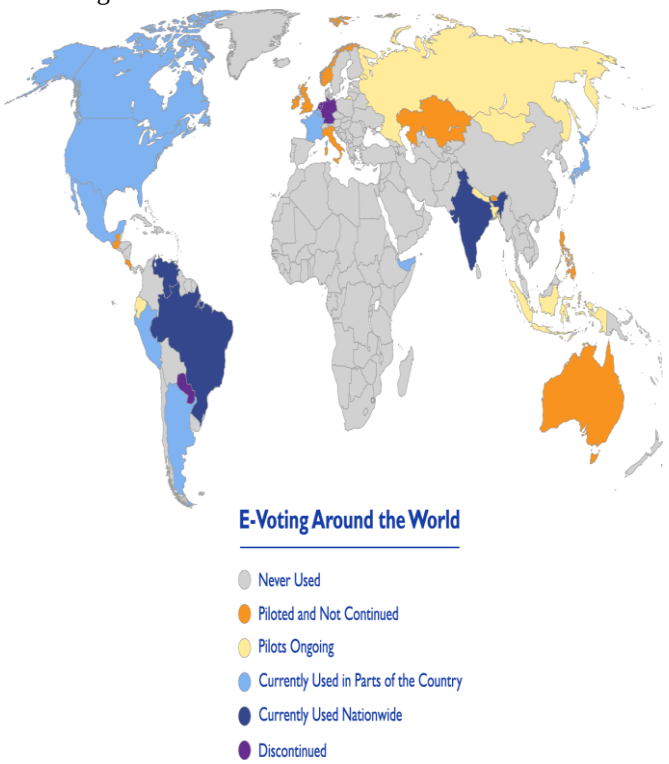
**N. Around World**

This guide will use the terminology “electronic voting and counting technologies.” As already demonstrated, there are a wide range of technology options covered by electronic voting and counting technologies. Suppliers also implement technologies in different ways, creating a confusing array of alternatives available to EMBs within and between these two broad categories. The variety of offered technologies might be one factor that has led to very different experiences in countries, which have used or attempted to use electronic voting and counting technologies.

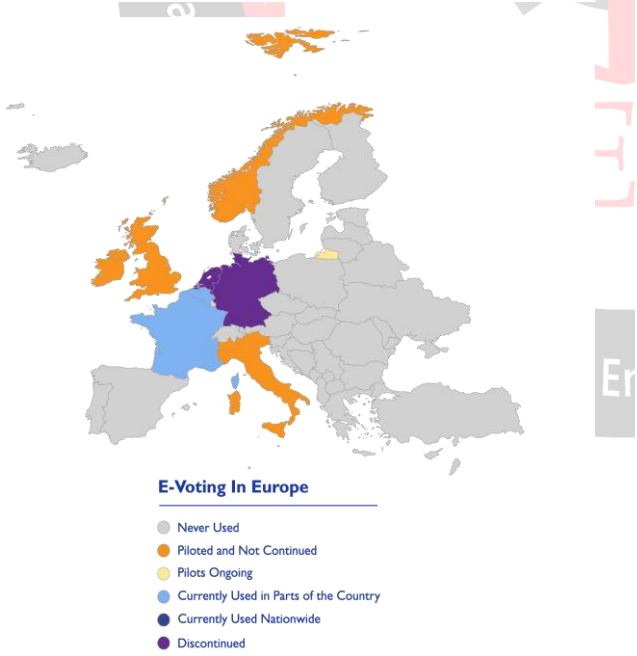
Voting technologies have a surprisingly long history. In the United States, mechanical lever voting machines were first used for elections in 1892 and were commonly used in U.S. elections until the 1990s. Electronic technologies began to appear in the 1960s with punch card counting machines. In the following decades, technologies such as DRE voting machines, ballot scanning machines and Internet voting began to appear. The U.S. was at the forefront of adopting many of these technologies. Through the 1990s and the first decade of the new millennium, an increasing number of countries around the world also started to adopt these

technologies.




Recent research has shown that 31 countries around the world have used non-remote electronic voting machines for binding political elections at some point. Some of these countries have experimented with EVMs and then decided not to continue with their use, in some cases after using them for many years. EVMs are being used in 20 countries, with **six of these countries still piloting the technology.** (https://www.ndi.org/sites/default/files/World-Evoting-Map%28150%29.png)




Globally, very different trends are seen in different regions. Europe and North America can be seen as moving away from the use of EVMs.

*(https://www.ndi.org/sites/default/files/Evoting-in-Europe%28150%29-01.png)*

*While Asia indicates expanding enthusiasm for utilizing electronic voting advances. Tragically, no comparable research is accessible for the worldwide utilization of electronic checking advances.*

## II. ANALYSIS AND DISCUSSION

### *A. Ballot system*

*Paper ballots are considered to be the most trustworthy methods to be used during an election but it comes with few limitations. We have listed down few disadvantages of the paper ballots due to which EVMs are preferred nowadays.*

There is no extension for automation in paper tally framework. Electronic voting machines are favored on the grounds that it diminishes the manual work and with one press of the catch, the votes are recorded. Post-race, it sets aside an enormous measure of opportunity to tally the votes previously pronouncing the outcomes. In electronic voting machines, the checking is being done inside couple of minutes. The general population who are physically tested think that its hard to cast their votes through the paper poll and regardless of whether they cast their votes utilizing paper ticket they expect somebody to make their choice for benefit. In such cases, their protection while making choice is broken. Be that as it may, with EVMs set up they can simply touch the screen so as to cast their votes by means of touch screen EVM. Paper is a substance that is inflammable subsequently in specific situations, the paper in which the votes were recorded in poll may get harmed then winds up plainly difficult to recover the records of the votes. Paper tickets can't be controlled however utilizing paper as a crude material in such voting framework it winds up noticeably destructive for the earth. Then again, utilizing electronic voting machines are significantly more conservative. In few spots where the administration is degenerate, they can without much of a stretch embed a few counterfeit paper votes in the tally and afterward it winds up noticeably difficult to track the legitimate votes. Hardly any electronic voting machines give paper trial for the votes recorded. Be that as it may, on the paper vote, there are no such affirmations. There is no automation set up which can tell that what number of votes was recorded every moment. Throwing votes utilizing paper vote is a tedious errand though voting by means of EVM is done in a couple of moment's seconds. The cost of use on the paper vote is path higher than on EVM. Utilizing EVMs are very sparing for the race commission. With the paper poll, the best test is that one would never utilize notable reference if there should be an occurrence of the paper tally while in EVMs one can store the records for a considerable length of time.

### *B. Internet Voting*

The most important issues to deal with Internet Voting is remote location, connectivity, hacking and voter's security and voting Ethics. A video link explaining why Internet voting is insecure is provided. This video, which is four minutes long and titled "Should We Trust Internet Voting?" is meant as a

high-level introduction to modern Internet voting schemes and the threats they face. This video is currently available online at www.youtube.com/watch?v=hg34L_iMg6s.

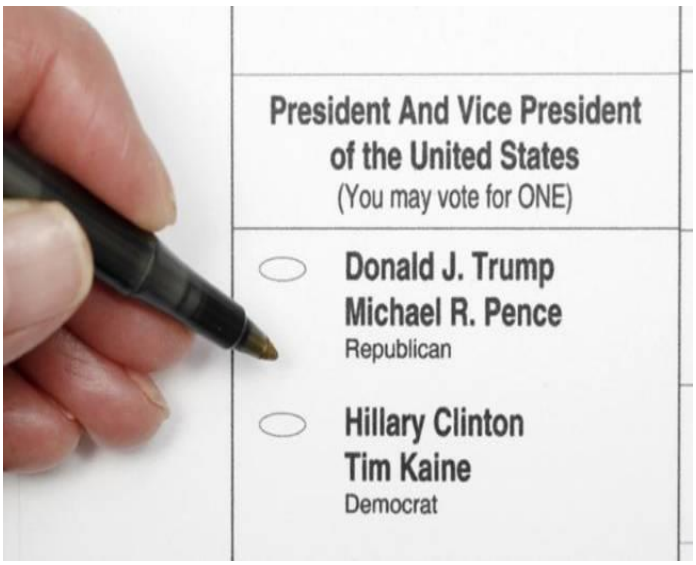
### *C. EVM and VVPATS*

Serious Issues of electronic voting can include viruses and hacking, as well physical tampering. Despite elaborate safeguards, India's EVMs are vulnerable to serious attacks. EVM software isn't safe. The electronic voting machines are safe and secure only if the source code used in the EVMs is genuine. Shockingly, the EVM manufacturers, the BEL and ECIL have shared the 'top secret' EVM software program with two foreign companies, Microchip (USA) and Renesas (Japan) to copy it onto microcontrollers used in EVMs. This process could have been done securely in-house by the Indian manufacturers. Worse, when the foreign companies deliver microcontrollers fused with software code to the EVM manufacturers, the EVM manufacturers cannot "read back" their contents as they are either OTP-ROM or masked chips. Amusingly, the software given to foreign companies is not even made available with the Election Commission, ostensibly for security reasons. With such ridiculous decisions, the Election Commission and the public sector manufacturers have rendered security of the EVMs a mockery. (GVL Narasimha Rao- http://www.indianevm.com/articles/ten-reasons-for-banning-indian-evms.pdf) EVM hardware isn't safe. The danger for EVM manipulations is not just from its software. Even the hardware isn't safe. Dr. Alex Halderman, professor of computer science in the University of Michigan says, "EVMs used in the West require software attacks as they are sophisticated voting machines and their hardware cannot be replaced cheaply. In contrast, the Indian EVMs can easily be replaced either in part or as wholesale units." One crucial part that can be faked is microcontrollers used in the EVMs in which the software is copied. EVM manufacturers have greatly facilitated fraud by using generic microcontrollers rather than more secure ASIC or FPGA microcontrollers. Not just only microcontrollers, mother boards (cards which contain microcontrollers) and entire EVMs can be replaced. Neither the Election Commission nor the manufacturers have undertaken any hardware or software audit till date. As a result, such manipulation attempts would go undetected. To detect such fraud, the upgraded EVMs have a provision to interface with an Authentication Unit that would allow the manufacturers to verify whether the EVM being used in the election is the same that they have supplied to the Election Commission. The EVM manufacturers developed an "Authentication Unit" engaging the services of Secure Spin, a Bangalore based software services firm. The Unit was developed and tested in 2006 but when the project was ready for implementation, the project was mysteriously shelved at the instance of the Election Commission. Several questions posed to the Election Commission for taking this decision went unanswered. The Indian EVMs can be hacked both before and after elections to alter election results. Apart from manipulating the EVM software and replacing many hardware parts discussed above, Indian EVMs can be hacked in many ways. To possibilities may be mentioned bellow. Each EVM contains two EEPROMs inside the Control Unit in which the voting data is stored. They are completely unsecured and the data inside EEPROMs can be manipulated from an external source. It is very easy to read (data from) the EEPROMs and manipulate them. The second and the most deadly way to hack Indian EVMs is by inserting a chip with Trojan inside the display section of the Control unit. This requires access to the EVM for just two minutes and these replacement units can be made for a few hundred rupees. Bypassing completely all inbuilt securities, this chip would manipulate the results and give out "fixed" results on the EVM screen. The Election Commission is completely oblivious to such possibilities. Contrary to claims by Indian election authorities, these paperless EVMs suffer from significant vulnerabilities. Even brief access to the machines could allow dishonest election "Insiders "or other criminals to alter election results. There are allegations that some "insiders" demanding vast sums (Rs. 5 Core or more for each assembly constituency) to fix election results. Who are these insiders? Unlike in the traditional ballot system where only the election officials were the "insiders", electronic voting machine regime has spawned a long chain of insiders, all of whom are outside the ambit and control of the Election Commission of India. There is every possibility that some of these "insiders" are involved in murky activities in fixing elections. The whole world—except us in India–is alive to the dangers of insider fraud in elections. The "insiders" include the public sector manufacturers of India's electronic voting machines namely, the Bharat Electronics Limited (BEL) and Electronics Corporation of India (ECIL), the foreign companies supplying microcontrollers, private players (some of which are allegedly owned by some political leaders) for carrying out checking and maintenance of electronic voting machines during elections. A team of researchers showed precisely how a display component could be replaced with a fake substitute programmed to steal a percentage of the votes in favor of a chosen candidate. They also demonstrated how stored votes could be changed between the election and the public counting session, which in India, can be weeks later, with a pocket-sized device. The team, comprising Hyderabad-based NetIndia, Dr J Alex Halderman, professor & noted expert on electronic voting security from the University of Michigan and Holland-based security expert Rop Gonggrijp, was instrumental in the ban on EVMs in the Netherlands. Which candidate to favor -Once the dishonest display is installed in an EVM (possibly months or years before the election), the attacker must communicate which candidate is to be favored or disfavored and by what margin. There are many different ways that attackers could send such a signal—various kinds of radios, secret combinations of key presses, or even by using the number of candidates on the ballot. Stealing of Votes to steal votes, the attacker indicates his favored candidate using the rotary switch, which selects a number from 0–9, and the attacker can use it to pick a favored candidate in any of the first 9 ballot positions, which

normally include the major national parties. When the switch is set to positions 1-9, the chip on the clip-on device executes a vote-stealing programmed. The programmed runs in two passes: first, it reads the list of votes and calculates how many votes to steal from each candidate, and second, it rewrites the list of votes, stealing votes as calculated in the first phase. Any time between the start of polling and the public count, dishonest election insiders or other criminals could use the clip-on device to change the votes recorded in the EVM. In India, counting sometimes takes place weeks after voting, so criminals could wait for an opportunity to tamper with the machines while they are in storage. In normal operation, the EVM limits the rate of voting to no more than 5 per minute. However, Clip-on device bypasses the software restrictions of the EVM, so an attacker is able to again forcibly take control of an EVM and stuff the electronic "ballot box" with any number of votes. These attacks are neither complicated nor difficult to perform, but they would be hard to detect or defend against. Dishonest insiders or other criminals with physical access to the machines at any time before ballots are counted can insert malicious hardware that can steal votes for the lifetime of the machines. Attackers with physical access between voting and counting can arbitrarily change vote totals and can learn which candidate each voter selected. The EVM has no means for the voter to verify that his/her votes have been tallied properly. The EVM has no means outside of the memories of the voting machines themselves to audit or recount the votes. Susceptibility to fraud: Although some may believe that tampering with an electronic voting machine is extremely hard to do, computer scientists have tampered with machines to prove that it is quite easily done. If people have access to the machines, and know how to work them, they can take the memory card out of the machine, which stores the votes, and in place they put their own memory card with a virus that can tamper with the votes. Government ties of manufacturers: The Government at the time of election may hire any manufacturer or company for manufacturing EVMs according to the needs of the political party in power An EVM can be tampered during manufacturing stage, that too during the manufacturing of the Chip. After tampering the EVM, it's difficult to detect it by a third party. When the tampering happens at the manufacturing stage of chip, even those who are assembling the EVMs will not be aware of and cannot detect tampering. Malicious software programming: Any computer software is basically generated from software programming and coding. And all these software could be tampered with by a computer programmer who knows the source code. Testing electronic voting systems is hard. If malicious coding is inserted by programmers into commercial software that are triggered by obscure combinations of commands and keystrokes via the computer keyboard, then election results can change completely. Physical security of machines: Secure storage of cast votes: The votes that are cast using the electronic voting machines are stored in a safe storage or space in the computer machine memory. The time gap between election and the counting of votes is a risk to possible hacking and manipulation. The chance of tampering increases as the time gap increases.

Why is America, a first-world country, still using paper ballots for the US Presidential Elections?




https://akm-img-a-in.tosshub.com/indiatoday/images/story/201611/voting647_110416083302.jpg

In two days, the United States of America with have a new President. High chances are that it will be either Hillary Clinton or Donald Trump. If surprise is in store for the world, then it could be Jill Stein or Gary Johnson, or even Evan McMullin. In fact, if a free-spirited, chicken-loving American citizen wants to vote for a KFC wing, they could do that too. Because even after over 15 years of debating over taking up electronic voting, America still uses the paper ballot system to elect their president.

***WHY IS THE PAPER BALLOT SYSTEM STILL PREVALENT IN THE US?***

(https://www.indiatoday.in/fyi/story/us-presidential-elections-paper-ballots-e-voting-350273-2016-11-04)

Security Reports have it that Americans feel safer in using paper ballots as compared to electronic voting machines, like Indians do. A TIME report quotes the US Election Assistance Commission Chairman Tom Hicks saying that the "primary reasons" paper ballots are used in most states are "security and voter preference". The report also says e-voting is not highly preferred because of the cost it comes with: the need for new voting machines, upgrades, are "greatly restricted by budget".

Another argument is that politicians would not got for e-voting over the dearly-known paper ballot ritual, which has been "accurately modeled from decades of polling and analysis". But here's the deal: considering that Americans use electronic gadgets for banking, educational purposes and even security, this logic may not stand tall for long.

***How Long Has The Paper Ballot Been Around In The Us?***

Printed ballots came into fashion in the US long after the American Revolutionary War, before which people cast their

votes by calling out their preferences in public. Most states had moved to secret ballots after 1884's presidential election of. By 1892, voting in private became prevalent. Printed ballots did not come into some seven states of America until the 20th century. Over the years, voting rights evolved in the US but so was not quite the case with the technology involved in voting. Hence, through the 1900s, forms of the paper ballot remained in fashion. Presently, though secret ballot is most prevalent across the US, some states use mail ballots. In this case, the ballot is sent to the voter's home, they mark their choice and mail it via post. Oregon and Washington conduct all elections by mailed ballots.

***E-VOTING IN THE US***

The only form of e-voting in the US is via email or fax. Technically, the voter is sent a ballot form; they fill it in, return it by email, or fax a digital photo of the ballot with their choice marked.

***CAN A VOTER VOTE FOR A NON-CANDIDATE IN THE PAPER BALLOTS?***

Say a voter writes Sheldon Cooper name on the ballot paper, and mark them for their presidential choice. They can do that. Known as a "write in" candidate, such unofficial candidates garner a lot of vote in American elections. A BBC report says that Mickey Mouse is an all-time favorite in the country. However, the odds of a write-in candidate becoming the US president are almost the same as the winning candidate "rowing across the Atlantic in a one-person rowboat and calling upon the Queen", says constitutional law expert Professor Rogers Smith.

***SO WHAT ARE THE CHANCES OF THE US GIVING UP ON PAPER BALLOTS?***

Based on what political scientists and various studies have to say, it is slim-to-none. A Scientific American report voices their fear of e-voting quite clearly: "No one has yet figured out a straightforward method of ensuring that one of the most revered democratic institutions - in this case, electing a US President - can be double-checked for fraud, particularly when paperless e-voting systems are used."

## III. PROPOSED SYSTEM

**Secure Manageable Automated Reliable Tamper-proof Voting System**

To ensure 100% voting automation came into play. But this automated system have been approved only on some developed countries since security have not been ensured to a large extent. Our main aim of the proposed system is to develop a compatible voting machine with high security. The proposed system is mainly designed for our country. The main objective of this project is to make authentication of voter more secure, powerful, realistic and to detect misleading of votes and prevent them. We can achieve this in two phases.

**Phase 1:- Smart Authentication**

First the details of the persons who are above 18 years are extracted from registered database. To ensure security, finger prints or retina scan or both of the voters is used as the main authentication resource. Since the finger pattern and retina of each human being is different, the voter can be easily authenticated. The system allows the voter to be identified uniquely through his fingerprint. This identification authenticates the voters and makes them eligible to cast vote. As soon as the voter casts a vote, voters name is fetched from registered database to our system and details which are identified are then tracked and will be locked to access(to ensure double voting fault).

**Phase 2:- Smart Voting**

EVM is tampered now days and votes are misleaded easily. To prevent this, a parallel hardware is developed. Hardware contains button inside it which are inaccessible to voter. This Hardware is connected to server. EVM machine is connected to the hardware. Hardware is connected to EVM machine by an object like a strip. At the time of vote casting EVM is used as the main machine to cast the vote. So when the button is pressed onto the EVM the strip connected to that particular button is pressed simultaneously onto the hardware. Therefore two separate results using single action is generated. Out of which one result is stored in EVM offline and another result is stored at secure server. After completion of voting process we are able to see whether there is misleaded of votes and also prevent it.

## V. CONCLUSION

Voting system is indeed serious issue upon which future of country is dependant. Different voting systems have different mechanism and functions, out of which most of the systems have failed to maintained the ethics and regulations of voting system and thus fail to complete the aim. So we introduce the smart and tampare-proof voting system, which will overcome real-time and most important issues in voting system.

**Advantages of Authentication Process**

Voter does not to carry any physical card for identification and voting. Accurate identification of voter is possible. Voter will not able to vote more than one time (Double Voting is Prevented).Voter cannot do fraud voting using different identity (Fake Voting is Prevented). We can identify the total number of voters who have and who haven't cast vote. We can send notification to that voter who hasn't cast their vote to inspire 100% voting.

**Advantage of Vote Casting Process**

Tampered and Faulty EVM machine can be detected. Misleads of vote can be prevented. More than one voting results to increase accuracy. Votes from different booth can be merged quickly. Result can be declared as soon as the voting if finished.

## Acknowledgement

We would like to express thanks of gratitude towards our guide Dr. Ayesha Butalia, HOD Shreekant Dhamdhere and our close supporters.

## REFERENCES

[1] "Audit of AEC'S electronics voting machine for blind and vision impaired voters", Technical Report by Australian Electoral Commission, 23 August 2007.

[2] Sarah P. Everett, Kristen K. Greene, Michael D. Byrne, Dan S. Wallach, Kyle Derr, Daniel Sandler and Ted Torous, "Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance", in the Proceedings of Measuring, Business, and Voting, Florence, Italy, April 5-10, 2008.

[3] Danny De Cock and Bart Preneel, "Electronic Voting in Belgium: Past and Future".

[4] Lorrie Faith Cranor, "Electronic Voting", Encyclopedia of Computers and Computer History, published by Fitzroy Dearborn, 2001.

[5] Kim Alexander, "Ten Things I Want People to Know About Voting Technology", California Voter Foundation, Presented to the Democracy Online Project's National Task Force, National Press Club, Washington, D. C., January 18, 2001.

[6] D. Jefferson, A.D. Rubin, B. Simons and D. Wagner, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", Technical Report by U.S. Department of Defense's FVAP (Federal Voting Assistance Program), January 05, 2004.

[7] T. Kohno, A. Stubblefield, A. D. Rubin and D. S. Wallach, "Analysis of an Electronic Voting System", IEEE Symposium on Security and Privacy 2004. IEEE Computer Society Press, May 2004.

[8] A.Ansper, A. Buldas, M. Oruaas, J. Piirsalu, A. Veldre, J. Willemson and K. Kivinurm, "The Security of Conception of E-Voting: Analysis and Measures", Technical Report by National Electoral Committee, 2002.

[9] "Online Voting", postnote – a publication of the U. K. Parliamentary Office of Science and Technology, May 2001.

[10] "HAND BOOK FOR POLLING AGENTS" (At Elections where Electronic Voting Machines are used), published by "Election Commission of India" in 2006.

[11] Thomos M.Buchsbaum, "E-Voting: International developments and lesson learnt", Technical Report by Australian Federal Ministry for Foreign Affairs, 2004.

[12] Belguim E-Voting system experiences difficulties. HTML Document.