Proceedings of the International Conference on
Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012

Electronic Voting Machine – A Review

D. Ashok Kumar
Department of Computer Science, Government Arts College, Trichy -22.
Tamilnadu, India.
Email: akudaiyar@yahoo.com

T. Ummal Sariba Begum
Department of Computer Science, Government Arts College, Trichy-22.
Tamilnadu, India.
Email: tummalsariba@gmail.com

Abstract— **Electronic Voting Machine (EVM) is a simple electronic device used to record votes in place of ballot papers and boxes which were used earlier in conventional voting system. Fundamental right to vote or simply voting in elections forms the basis of democracy. All earlier elections be it state elections or centre elections a voter used to cast his/her favorite candidate by putting the stamp against his/her name and then folding the ballot paper as per a prescribed method before putting it in the Ballot Box. This is a long, time-consuming process and very much prone to errors. This situation continued till election scene was completely changed by electronic voting machine. No more ballot paper, ballot boxes, stamping, etc. all this condensed into a simple box called ballot unit of the electronic voting machine. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token or knowledge based methods. So the Electronic voting system has to be improved based on the current technologies viz., biometric system. This article discusses complete review about voting devices, Issues and comparison among the voting methods and biometric EVM.**

Keywords- ***Voting, Electronic Voting Machine (EVM), Biometric EVM.***

I. INTRODUCTION

Elections allow the populace to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election.

This paper presents a survey of the state of the art in Electronic Voting, including the various works done in Internet Voting and the arguments against its use, as well as in electronic poll-site voting. Electronic voting refers to the use of computers or computerized voting equipment to cast ballots in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Electronic systems can be used to register voters, tally ballots, and record votes [11].

The design of a "good" voting system, whether electronic or using traditional paper ballots or mechanical devices must satisfy a number of competing criteria. The *anonymity* of a voter's ballot must be preserved, both to guarantee the voter's safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes. The *existence* of such evidence would allow votes to be purchased by a candidate. The voting system must also be *tamper-resistant* to thwart a wide range of attacks, including ballot stuffing by votes and incorrect tallying by insiders.

Electronic Voting Systems: There have been several studies on using computer technologies to improve elections [3, 20, 12, 14, and 16]. These studies caution against the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. Electronic voting machine is a simple machine that can be operated easily by both the polling personnel and the voters. Being a standalone machine without any network connectivity, nobody can interfere with its programming and manipulate the result. Keeping the erratic power supply position in many places in the country, the machines have been made to run on batteries. It has mainly two units: Control unit and Ballot unit. The Control Unit is the main unit which stores all data and controls the functioning of EVM. The program which controls the functioning of the control unit is burnt into a micro chip on a "one time programmable basis". Once burnt it cannot be read, copied out or altered. The EVMs use dynamic coding to enhance security of data transmitted from ballot unit to control unit.

Although there has been cryptographic research on electronic voting [7], and there are new approaches such as [4] currently the most viable solution for securing electronic voting machines is to introduce a "voter-verifiable audit trail" [6, 12]. A verifiable audit trail does not, by itself, address voter privacy concerns, ballot stuffing, or numerous other attacks on elections. Some vendors have claimed "security through obscurity" as a defense, despite the security community's universally held belief in the inadequacy of obscurity to provide meaningful protection. [4].

Electronic voting: It is also known as **e-voting** is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. Electronic voting technology can include punched cards, optical scan voting systems and specialized

978-1-4673-1039-0/12/$31.00 ©2012 IEEE

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. And, of course, EVM helps maintain total voting secrecy without the use of ballot papers. And, at the end of the polling, just press a button and there you have the results.

India's experience in e voting: India is the world's largest democracy with a population of more than one billion. India has an electorate of more than 668 million and covers 543 parliamentary constituencies. Voting is the bridge between the governed and government. In previous manual elections in India, a nationwide ballot could consume around 8,000 tons of paper and 400,000 phials of indelible ink and require some 2.5 million strongboxes to store them under heavy security until the votes were counted. In the past, it took up to three or four days to count the votes, with hired personnel spending day and night in secured areas manually counting each ballot. Sometimes demanding for recounting resulting for the low margin of difference of votes between the top two candidates coupled with large number of invalid and doubtful votes [17]. The electronic voting machines are intended both to reduce errors and to speed the counting process. The country developed its electronic voting machines (EVM) through an indigenous technology. It was designed by Bharat Electronic Ltd, and the Electronics Corporation of India Ltd, with the microchip imported from Japan. The country developed over one million EVM s for its 668 million voters. It would have cost them a great deal of money. The machine was able to Cater for 64 candidates per election, in pages of 16 candidates each. The technology was able to solve a lot of problems associated with the traditional voting system. However, before its adoption there were pilot schemes in five states to familiarize the voters with the technology.

PROPERTIES OF EVM: Researchers in the electronic voting field have already reached a consensus pack of following core properties that an electronic voting system should have [16]:

Accuracy: (1) it is not possible for a vote to be altered, (2) it is not possible for a validated vote to be eliminated from the final tally, and (3) it is not possible for an invalid vote to be counted in the final tally.

Democracy: (1) it permits only eligible voters to vote and, (2) it ensures that eligible voters vote only once.

Privacy: (1) neither authorities nor anyone else can link any ballot to the voter who cast it and (2) no voter can prove that he voted in a particular way.

Verifiability: anyone can independently verify that all votes have been counted correctly.

Availability: (1) the system works properly as long as the poll stands and (2) any voter can have access to it from the beginning to the end of the poll.

Resume Ability: the system allows any voter who had interrupted his/her voting process to resume it or restart it while the poll stands.

II. TAXONOMY OF VOTING DEVICES

There are different forms of Electronic Voting Machines are used in across the world. The variations of EVM are as follows:

A. Paper-based electronic voting system

Sometimes called a "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. Most recently, these systems can include an Electronic Ballot Marker (EBM), that allow voters to make their selections using an electronic input device, usually a touch screen system similar to a Direct-recording electronic (DRE). Systems including a ballot marking device can incorporate different forms of assistive technology.

B. Direct-recording electronic (DRE) voting system

Electronic voting machine by Premier Election Solutions formerly Diebold Election Systems used in all Brazilian elections.

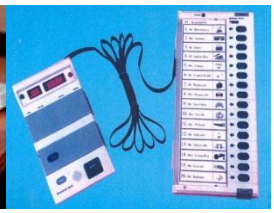

Fig.1. DRE Voting system (Left) Fig 2. Indian Voting Machine (Right)

A DRE voting machine in Fig.1 records votes by means of a ballot display provided with mechanical or electro-optical components that can be activated by the voter (typically buttons or a touch screen); that processes data with computer software; and that records voting data and ballot images in memory components. After the election it produces a tabulation of the voting data stored in a removable memory component and as printed copy. The system may also provide a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting results from precincts at the central location. These systems use a precinct count method that tabulates ballots at the polling place. They typically tabulate ballots as they are cast and print the results after the close of polling document. Please do not revise any of the current designations.

C. Indian EVM Device

India is world's largest democracy. It is perceived to be charismatic one as it accommodates cultural, regional, economical, social disparities and still is able to stand on its own. In 2004, India had adopted Electronic Voting Machines for its elections to the Parliament with 380 million voters had cast their ballots using more than a million voting machines. The Indian EVMs are designed and developed by two

Government Owned Defense Equipment Manufacturing Units, Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited (ECIL). Both systems are identical, and are developed to the specifications of Election Commission of India. The System is a set of two devices running on 6V batteries.

One device, the Voting Unit is used by the Voter, and another device called the Control Unit is operated by the Electoral Officer. Both units are connected by a 5 meter cable (Fig.2). The Voting unit has a Blue Button for every candidate, the unit can hold 16 candidates, but up to 4 units can be chained, to accommodate 64 candidates. The Control Units has three buttons on the surface, namely, one button to release a single vote, one button to see the total number of vote cast till now, and one button to close the election process. The result button is hidden and sealed; it cannot be pressed unless the Close button is already pressed.

D. 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. Vote data may be transmitted as individual ballots as they are cast, periodically as batches of ballots throughout the Election Day, or as one batch at the close of voting. This includes Internet voting as well as telephone voting. Public network DRE voting system can utilize either precinct count or central count method. The central count method tabulates ballots from multiple precincts at a central location.

E. Diebold AccuVote-TS

The Diebold AccuVote machine is the system that tested [2], and is in use in the State of Maryland. It uses a touch screen (Fig. 3) with a card reader that the voter gets after being authenticated by polling officials.

Fig 3: Diebold AccuVote-TS system (Left) and Hart InterCivc eSlate system (Right)

Indeed, the CVS source code repository for Diebold's AccuVote-TS DRE voting system recently appeared on the Internet [18]. This appearance, announced by Bev Harris and discussed in their book, Black Box Voting [8], gives us a unique opportunity to analyze a widely used, paperless DRE system and evaluate the manufacture's security claims. Jones discusses the origins of this code in extensive details [9]. Diebold's voting systems are in use in 37 states, and they are the second largest and the fastest growing vendor of electronic voting machines. And also only inspected unencrypted source code, focusing on the AVTSCE, or AccuVote-TS version 4, tree in the CVS repository. This tree has entries dating from October 2000 and culminates in an April 2002 snapshot of version 4.3.1 of the AccuVote-TS system. From the comments in the CVS logs, the AccuVote-TS version 4 tree is an import of an earlier AccuTouch-CE tree. They did not have source code to Diebold's GEMS back-end election management system.

A group led by Avi Rubin analyzed the Diebold AccuVote TS DRE voting machine and found numerous flaws [18]. SAIC was commissions by the state of Maryland to do another analysis of the Diebold voting system and found the system, as implemented in policy, procedure, and technology, is at high risk of compromise. Based on these reports, the California Secretary of State's office established security procedures for DRE voting machine. Diebold used uncertified software in their electronic voting equipment in California. Diebold was then banned from California elections by the California Secretary of State.

F. Hart InterCivic eSlate

The Hart InterCivic eSlate (Fig. 3) is a hardware-based voting device with no touch screen [2]. It displays the ballot in a page-at-once format (displaying multiple races on one page). Voters navigate using triangle-shaped "prev" and "next" keys. Voting itself is accomplished by rotating a dial labeled "select" until the desired candidate is highlighted. To vote, the "enter" key is pressed. After all votes have been entered, the user presses the red "cast ballot" key.

G. SureVote

The SureVote Company provides a system that offers higher protection against malfunction or fraud (Fig 4). At voting time, users authenticate themselves and their right to vote using a numeric personal identification code and a numeric ballot code [2]. They then can enter a four-digit "vote code" for each race. An error message is presented if the entered code is invalid for that race. If the code is valid, the vote is sent to multiple vote storage servers scattered across the country. Each server sends back a numeric response, which is combined by the client into another four-digit code, the "sure code".

H. VoteHere Platinum

VoteHere Platinum [2] uses a completely software-based touch screen interface. It can be run on any personal computer with a touch screen monitor. However, this also means that the system does not offer hardware buttons or any of the benefits that Hardware buttons provide. In addition, it introduces new risks that the computer the software is running on may have been tampered with the Vote Here system presents one race on the screen at a time; the voter presses the "next" and "back"

buttons at the top of the screen to navigate between races (Fig 5).

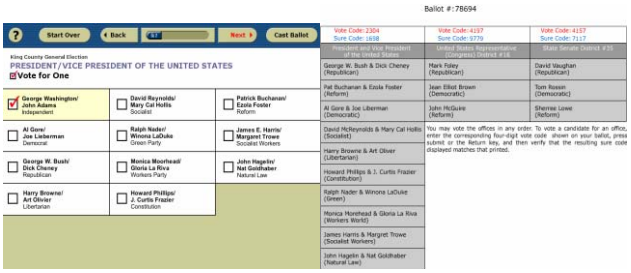

Fig 4: SureVote DRE system((Left) Fig 5: VoteHere Platinum System(Right)

I. *Biometric EVM*

Biometrics refers to an automated system that can identify an individual by measuring their physical and behavioral uniqueness or patterns, and comparing it to those on record. In other words, instead of requesting personal identification cards, magnetic cards, keys or passwords, biometrics can identify fingerprints, face, iris, palm prints, signature, DNA, or retinas of an individual for easy and convenient verification. With the boom in Internet-based business and the increased need for accurate verification when accessing accounts, biometrics is the simplest and most convenient the solution. Biometrics can also provide you with convenience and security, by enabling a machine to verify the individual by itself and to respond to the individual's requests.

The objectives of biometric recognition are user convenience (e.g., money withdrawal without ATM card or PIN), better security (e.g., difficult to forge access), and higher efficiency (e.g., lower overhead for computer password maintenance). The tremendous success of fingerprint based recognition technology in law enforcement applications, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all ushered in an era of fingerprint-based person recognition applications in commercial, civilian, and financial domains. So the EVM has to be improved based on the current technologies viz, biometric system.

Some previous work use fingerprint for the purpose of voter identification or authentication. As the fingerprint of every individual is unique, it helps in maximizing the accuracy. A database is created containing the fingerprint of all the voters in the constituency. Illegal votes and repetition of votes is checked for in this system. Hence if this system is employed the elections would be fair and free from rigging.

A fingerprint identification system should be used which can: 1) store the fingerprint of a person at some given time. 2) Should recognize whether the prints match or not at some other instant of time. 3) It should be touch sensitive; thumb prints are stored when a person places his thumb on a particular area & they are recognized at a later instant. The mechanism of working is: Centers for recording thumb prints must be installed two months before voting. Here persons register their prints. During the actual voting, the voter first places his thumb on the touch sensitive region. If the print matches he is allowed to vote. In case the print is not stored before, a single beep is given, so the person cannot vote OR if the same person votes again, the system should give a double beep, so that the security can be alerted. The system is programmed to recognize a print twice, but to give a beep for more than once [1]. The comparison of Paper voting, Diebold and Biometric EVM are shown in the Table 1.

J. *Comparison among the countries of electronic voting system*

The last few years have brought a renewed focus on to the technology used in the voting process. The current voting system has many security holes, and it is difficult to prove even simple security properties about them. The comparison between EVM and computerized EVM is shown in the Table 2. A voting system that can be proven correct has many concerns. There are some reasons for a government to use electronic systems are to increase elections activities and to reduce the elections expenses. Still there is some scope of work in electronic voting system because there is no way of identification by the electronic voting system whether the user is authentic or not and securing electronic voting machine from miscreants. The following Table 3 provides an overview of the experiences of other countries using electronic voting machine [17]. The comparative focus is on the adoption of electronic voting systems adopted at the international level.

III. ISSUES OF EVM

Around the world, electoral officials are examining various technologies to address a wide ranging array of voting issues like [13]: System adaptability and acceptability by all stockholders including common People residing in remote villages, probably some of them illiterate too. System functionality as close to conventional ballot paper system as possible. Cost effectiveness and ease of deployment / maintenance of the system. System reliability and security in terms of tamper resistance, errors free operation etc., Speed and efficiency of voting and results declaration.

A. *Accessibility*

One of the largest issues related to DRE voting systems is accessibility [2]. For designers of computer programs, accessibility is the easiest design factor to ignore. Many classes of voters can easily be disenfranchised by a voting system that accommodates only "normal" users. The most obvious of these is disabled voters. The federal **V**oting **A**ccessibility for the **E**lderly and **H**andicapped **A**ct (VAEHA), passed in 1984, mandates that polling places be available and usable by the elderly and handicapped [19]. According to the National Organization on Disability, DRE balloting systems are the most accessible technology, compared to lever, punch-card, optical scan, and hand count systems [21].

B. Age and Technical Experience

In addition to general disabilities, the issue of "computer disability" can cause problems in DRE Elections [2]. Research suggests that older adults consistently perform more poorly than younger adults in performing computer-based tasks. This is true both with respect to the amount of time required to perform the task, as well as the number of errors made [10]. In one recent study, age was positively correlated with difficulty in performing tasks with a computer mouse [15]. Although popular DRE systems do not use a computer mouse, similar issues are present. Older adults have greater difficulty in viewing a computer screen, and correct conceptualization of the relationship between screen or button manipulation and program activity may be a problem [13].

TABLE: 2 COMPARISONS OF EVM AND COMPUTERIZED EVM

S.No	EVM's of BEL	Computerized Voting Systems
1	Customized and proprietary hardware and software	Commercial, general purpose hardware & Operating system.
2	Software fused permanently in Integrated Circuits; cannot be accessed, retrieved or altered.	Software written in C, C++ etc which are unsafe for such applications and resident in Flash memories, which can be manipulated
3	The unique signature of every controller used in the machine is checked for authenticity, generating evidences if tampered with.	General purpose Method Board architecture do not provide such unique features.
4	Voting data reside in double redundant EEPROMs; do not need any external back up battery for retention	Voting data generally resides in RAM with battery back up on Mother Boards wand are vulnerable for corruption if battery fails.
5	Very similar in concept to the conventional voting, Ballot Unit replaces the Ballot Paper; Control Unit replaces the Ballot Box. Minimum change by automation	Conceptually very drastic change, ignores human metaphor, leads to low confidence level for a common voter.
6	Very low investment in awareness campaigns and training.	Being based on computers, voters need to be educated elaborately, high cost of training
7	Easy transportation, set up and operation, operates on battery. Very low Mean Time Between Failure (MTBF), more than 10 years of guaranteed life cycle, simple maintenance Cost of Ownership is extremely low.	Mains operated, back up by UPS. Transportation and set up costs are relatively high Cost of ownership is high

C. Bias

Aside from accessibility, the issue of bias presents both a logistical and a legal problem for elections [2]. Actual ballot design is fairly contentious, in part, because candidates believe that their location on the ballot changes the likelihood that a voter will select them. For example, candidates listed first on a ballot are generally favored [5]. For this reason, many jurisdictions pre-select a designated balloting order; often, candidates are listed by party in a specified configuration, by lottery, or alphabetically. Electronic ballots cannot avoid these pitfalls for the same reason that paper ballots cannot; names on a ballot must be presented in some fashion.

D. Accountability and Verifiability

Traditionally, votes were cast on paper and counted by hand [2]. Voters were confident that the marks they made on ballots reflected their intended vote. Voting machines that used levers and punch card systems also provided voters with a high degree of confidence that they cast their votes as intended. Until the 2000 elections voters also routinely assumed their votes were properly counted. The most pressing verifiability problem with the use of computerized voting is that the systems are provided by private companies, and the government usually has no oversight into the production of the systems beyond choosing whether or not to use them.

IV. NEED FOR FURTHER DEVELOPMENT

- Since the EVM Design is suitable for electoral system of any country, it need slight modifications.
- The authentication has to be extended in to second level (first level with VOTER ID) either by using thumb impression or by iris technology, so that one can avoid polling agents and casting vote by unauthorized voters.
- When the current EVM technology is innovated with networking capabilities, one can vote from anywhere in the world from any internet center provided with thumb impression/Iris device on the same day. Those network of Biometric EVM has to be developed for security as well as to get the result as fast as when the election gets over so that the Election day itself we get the result.
- The EVM software developed with minor modifications will favor the conduct of elections for both assembly and the parliament at the same time and it can also use for local body elections.
- The EVM has to be designed for addressing larger population so that we can conduct election for entire country without any day intervals.

V. CONCLUSION

This review discussed introduction about EVM and its variation, Issues of EVM, Taxonomy, and Biometric based EVM. Our efforts to understand electronic voting systems leave us optimistic, but concerned. This paper suggest that the EVM system has to be further studied and innovated to reach all level of community, so that the voter confidence will increase and election officials will make more involvement in purchasing the innovated EVM's for conduct smooth, secure, tamper- resistant Elections.

ACKNOWLEDGMENT

This work is a part of a Major Research Project and authors are thankful to UGC for funding the Project (File No. F-38-258/2009 (SR) Dt: 19.12.2009).The authors would like to

thank the anonymous reviewers for their thorough reviews, and constructive suggestions which significantly enhance the presentation of the paper.

REFERENCES

[1] Ashok Kumar D., Ummal Sariba Begum T., "A Novel design of Electronic Voting System Using Fingerprint", International Journal of Innovative Technology & Creative Engineering (ISSN:2045-8711),Vol.1,No.1. pp: 12 19, January 2011.

[2] Benjamin B., Bederson, Bongshin Lee., Robert M. Sherman., Paul S., Herrnson, Richard G. Niemi., "Electronic Voting System Usability Issues**",** In Proceedings of the SIGCHI conference on Human factors in computing systems, 2003.

[3] California Internet Voting Task Force. "A Report on the Feasibility of Internet Voting", Jan.2000.

[4] Chaum D., "Secret-ballot receipts: True voter-verifiable elections", IEEE Security and Privacy, 2(1):38-47, 2004.

[5] Darcy, R., & McAllister, I., "Ballot Position Effects", Electoral Studies*,* *9*(1), pp.5-17, 1990.

[6] Dill D.L., Mercuri R., Neumann P.G., and Wallach D.S., "Frequently Asked Questions about DRE Voting Systems", Feb.2003.

[7] Gritzalis D., [Editor]., "Secure Electronic Voting", Springer-Verlag, Berlin Germany, 2003.

[8] Harris B., "Balck Box Voting: Vote Tampering in the 21st Century", Elon House/Plan Nine, July 2003.

[9] Jones D. W., "The case of the DieboldFTP Site", THE UNIVERSITY OF IOWA Department of Computer Science, July 2003.

[10] Kubeck, J. E., Delp, N. D., Haslett, T. K., & McDaniel, M. "A Does Job- Related Training Performance Decline With Age? Psychology and Aging", 11, pp.92-107, 1996.

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

[12] Mercuri, R., "Electronic Vote Tabulation Checks and balances", PhD thesis, University of Pennsylvania, Philadelphia, PA, Oct.2000.

[13] NAACP Philadelphia Branch, et al. v. Ridge, et al. EXIS 11520. U.S. District Court, 2000.

[14] National Science Foundation. Report on the National Workshop on Internet Voting: Issues and Research Agenda, Mar.2001.

[15] Riviere, C. N., & Thakor, N. V., "Effects of Age and Disability on Tracking Tasks with a Computer Mouse: Accuracy and Linearity", Journal of Rehabilitation Research and Development, *33*, pp. 6-16, 1996.

[16] Rubin A.D. "Security considerations for remote electronic voting", ACM, 5(12):39-44, Dec.2002.

[17] Sanjay Kumar, Dr. Ekta Waliam., "Analysis of Electronic Voting System in Various Countries", International Journal on Computer Science and Engineering (IJCSE)", ISSN: 0975-3397 Vol. 3 No. 5 May 2011.

[18] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, " Analysis of an Electronic voting System", In Proc. IEEE Symposium on Security and Privacy, May , 2004.

[19] "Voting Accessibility for the Elderly and Handicapped Act"., Public Law 98-435 oversight hearing before the Subcommittee on Elections of the Committee on House Administration, House of Representatives, One Hundred Third Congress, second session., September 13, 1994

[20] "Voting: What Is; What Could Be"., Caltech/MIT Voting Technology Project., July 2001.

[21] "Voting System Accessibility Comparison", National Organization on Disability, Washington, DC, 2001

TABLE 1: COMPARE AND CONTRAST: PAPER VOTING, EVM, DIEBOLD AND BIOMETRIC EVM

S. No	**Differs in**	**Ballot Paper**	**EVM**	**Diebold**	**Biometric EVM**
1	Device Type	Papers and boxes	Embedded system with Assembly code	Embedded system with Windows CE, and C++ code	Embedded system with Assembly code
2	Visual Output	Stamp on paper	Single LED against each candidate's name	Color Touch screen, with GUI Software	Single LED against each candidate's name
3	Operating System/Software	No Operating System	None, the Assemble code to register number of votes is all it has. Hence it is simple automation of voting, no complexities	Windows CE and C++ code stored on the Internal Memory and PCMCIA cards, bulky, unnecessary additions.	None, the Assemble code to register number of votes is all it has. Hence it is simple automation of voting, no complexities
4	Records/Audits	Manual counting to be done by officials, lengthy, time consuming process, Inaccurate due to human errors	The Voting unit doesn't store anything, the control unit records the number of votes case for each candidate against his serial number. No record to link person-to-vote	Internal ribbon printer. And PCMCIS storage for records and audit trials. Additionally the GEMS server also stores the votes and audits. Again unnecessary addition, work can be accomplished by simple counter.	The Voting unit doesn't store anything, the control unit records the number of votes cast for each candidate against his serial number.

5	Control and Operation	Manual Operation	Automatic operation, The control unit accumulates the votes; it is a device with flash storage and seven segment LED display. The ballot unit has a button to issue a ballot for a voter	Complex automatic operation. Two GEMS servers one primary and a backup, for every polling station, that connects to the voting units to "Load the ballots" an then voting units work independently	Automatic operation, The control unit accumulates the votes; it is a device with flash storage and seven segment LED display. The ballot unit has a button to issue a ballot for a voter
6	Security Issues	No security provided by the system, neither during polling nor during voting	During polling, a facility is provided to seal the machine in case of booth capturing. No further voting can be done afterwards	GEMS server has access through Supervisory Smart cards, and PINS, some users have login and password access. But these server connections can be easily tapped and can be used for tempering with the data or procedure.	During polling, the voters' biometric trait is checked between the control and ballot unit. Once both measures are matched then only allow the person to cast a vote. And also once polling gets over, a facility is provided to seal the machine in case of booth capturing. No further voting can be done afterwards
7	Ballot Issue	Ballot paper is issued by Electoral officer on which voter could cast his vote	Ballot is issued by Electoral officer by pressing a button on the control unit. It allows the voter to press any button on the ballot unit to cast is vote	Voter access smart card is issued in an envelope for a terminal. Voter can put it in the assigned terminal and cast his/her vote. This smart card system rarely uses encryption and hence it is not difficult to duplicate these cards and pose false identity.	Ballot is issued by Electoral officer by pressing a button on the control unit. Once the person pressed his/her biometric trait compared with the stored information which is in the memory card, it allows the voter to press any button on the ballot unit to cast his vote
8	Storage of Votes	In ballot boxes assigned for the purpose of storing votes, highly insecure method of storage	In internal Non removable memory of the control units. No transfer over network. Security increased with this failure. Moreover these results can't be accessed by authorized personnel only at commissioned offices.	In a PCMCIA card hidden in the Voting Unit. Results are "transmitted" using modems to the counting center. Transmitting data over network is very risky, not the best means of result.	The details about the voters are stored in a Read only memory card and it is in the control unit. Moreover these results can't be accessed by authorized personnel only at commissioned offices.
9	Cost of the System	High cost of paper printing in millions an low speed of the whole process	About 12000 INR (300$) for one EVM	About 3300$	About 100000 (INR) for one EVM
10	Power Supply	No power supply required	6V alkaline batteries or electricity	Only electricity means, system will crash in case of power failure.	6V alkaline batteries or electricity
11	Capacity	As much a ballot box can hold	3840 Votes	Over 35000 votes.	3840 Votes

TABLE: 3 COMPARISONS AMONG THE COUNTRIES OF EVM

Country	E-Voting	Company	Election Type	Electoral System	Introduced Year	Year Used	Software Used	Hardware Used	Problems
India	668 Million	BHEL	State	FPP	2001	2009/2004 /2003/2001	EPROM	EVM	None
Brazil	66 million	UniSys & Diebold	All Govt Level	-	1996	1996/1998 /2000/2002	GEMS	GX-1 Integrated Processor	None
Belgium	3.2 Million	Steria	General & Municipal	Open PR-List	1994	1999	Digivote, Jites Stesud	DEVS	2003:500 Power And Computer Failure
Australia	218000	Software Improve	ACT Federal	PR-STV	2001	2001	eVACS	PCs	None
UK	1.5 Million	SVS	Local Govt	FPP	2000	2000/2003	AVC	DRE	Mobile e Voting
Spain	3000	Indra	Municipal	PR-List	2002	2003	SIRE	SIRE System	None
Canada	98000	CanVote	Municipal	FPP	2002	2003	CanVote On Linux	CanVote Internet	None