Review of Literature

Kilian Joseph John (2000) – In this patent the inventor has given a secure receipt-free voting scheme that is described where each voter does not leave evidence of how the voter voted by using a physically secure untappable channel. The term “secure untappable channel” refers to the fact that a message can be sent from a centre without being accessed or detected by another party. The end result of using an untappable channel is that neither the voter nor another party can show or prove how a vote was cast or what the message that was sent. Once a message is sent or received, the content may be changed rendering proof of the message impossible. However, if the message is intercepted it will be detected in route or at the time of reception. Moreover, even if a non-secure channel is used, if the message travels along the channel without interruption or detection, by virtue of the protocol used in the present invention, determination of a particular vote after receipt at its destination is not possible. In other Words, an untappable channel refers to the transmission of a message without interception or detection in route.

Bannet Jonathan et al. (2003) – This article presents a research voting system and associated class project which was used to demonstrate several classes of bugs that might occur in such a voting system unbeknownst to voters, with the difficulty of detecting these bugs through auditing. The intent of this project is to justify the mistrust sometimes placed in DRE voting systems that lack a Voter- Verifiable Audit Trail. The direct recording electronic (DRE) voting systems have some usability advantages over traditional systems, they raise serious security concerns. The authors shown, using a “toy” voting system called Hack-a-Vote, how easily a purely electronic voting system can be compromised and how difficult it can be for auditors to identify and correct any “hacks” in the voting system, any of which could otherwise completely compromise the results of an election.

Riza Aditya et al. (2004) – States in their paper as cheating is an inherent threat to voting, it is essential that an e-voting system provides a high level of
security. At the moment, commercially available e-voting solutions mainly advertise their convenience, efficiency and low cost. On the other hand, cryptographically secure voting schemes in the literature are generally considered to be complex and inefficient for a real-world implementation. This paper examines implementation issues of cryptographically secure secret-ballot voting schemes. A survey of different schemes and various implementations was provided. The possibilities of hardware implementations for various cryptographic primitives are discussed. The paper provides a foundation in designing secure and practical e-voting schemes to produce a secure, efficient and publicly acceptable implementation of voting schemes in the real world. Implementing a sound and secure e-voting system is not as straightforward as simply employing counting software. Accuracy, privacy, receipt-freeness, eligibility, prevention of double voting, fairness, robustness and verifiability/accountability are security requirements that an e-voting system must address.

**Kargel David (2004)** - In this patent the inventor has given a method for conducting an election among a plurality of voters includes the steps of: providing each voter with a ballot having at least one unique identifying symbol and a section for authenticating a voting selection; retaining a record of each voting selection; publishing the record of each voting selection; validating the published record of each voting selection; tabulating the voting selections from the validated record; and certifying the tabulated voting selections. The present invention provides a method and system that standardizes and improves the task of ensuring an accurate vote reception and count. The major components of the method involve providing ballots to a group of voters; recording votes from the group of voters; publishing the votes from the group; validating the published votes on a per-voter basis; tabulating the votes validated; and certifying that the tabulated votes were accurately counted.

**Chung Kevin KwongTai et al. (2005)** - The inventor had given a foolproof system for the purpose of voting this machine is readable ballot comprises a ballot sheet having a voting identifier including a representation of election...
jurisdiction information and a unique ballot identifier. A plurality of contest regions each has two or more mark spaces for making voting selections. The present invention relates to a voting apparatus and method and, in particular, to voting apparatus and method employing an optically read ballot. Under current election law and regulations in certain jurisdictions, a paper record of certain voter’s voting selections must be made and preserved. Most commonly, a paper voting record or ballot must be utilized for absentee voting and/or for provisional voting. Absentee voting is Where a voter Who Will be absent from the jurisdiction or otherwise unable to be present at a designated polling location during the time for voting is issued a paper ballot in advance of the election and votes by completing and submitting the paper absentee ballot by hand, mail, messenger, or other permitted means. Provisional voting is Where a voter who is unable to establish his eligibility to vote at a polling place during an election is issued a paper ballot and is permitted to vote thereby “provisionally,” i.e. by sealed paper provisional ballot that is only opened and counted if the eligibility of the provisional voter to vote is established by election officials after the time for voting ends.

Anand Ashish et al. (2007) – In the paper Evolutionary Enhancements of e-Voting Technology the authors states E-Voting being a complex social, political, legal & technical issue that requires a novel approach to make elections cheaper, scalable with growing population, enhance quality of national elections, maximizing public trust. Though there are known ways of detecting bogus & false voting, such methods should be free from voting secrecy intrusion, privacy intrusion and identity-leak possibilities. Technical issues of e-voting platform security remain a central concern in addition to tamper-proof being replication-proof along with public verifiability and accountability as key issue. Another aspect of this paper is about novel method of post-poll authentic repudiation of false voting. Minimizing human factor, discretionary powers and ensuring 360 degree accountability for all stakeholders in a democracy is desired. This paper proposes a unified, novel but small solution for a big vision. This scheme provides each e-Voting platform unique credentials at hardware, software and platform uniqueness originalities.
Yasinsac Alec et al. (2007) – In this report the authors basically focuses on conducting a scientifically rigorous static software analysis on the iVotronics version 8.0.1.2 firmware source code to determine and identify flaws, vulnerabilities or anomalies, if any, that may have potentially caused, contributed or otherwise created the higher than expected under-vote rate in the District 13 Race. The team’s unanimous opinion is that the iVotronic firmware, including faults that they identified, They traced program execution from terminal initialization, through voter selection, to ballot image creation, to ballot image collection. They also investigated the possibility of synchronous system faults not associated with any particular phase of voting. Their investigation provided no evidence that an iVotronic software malfunction caused or contributed.

Enguehard Chantal (2008) - In this paper author determined whether electronic voting can simultaneously protect secrecy, be transparent, accessible and resistant to intimidation and fraud. He considers different types of e-voting ranging from Direct Recording Electronic voting systems to remote internet voting. he showed that there are major contradictions between the constraints of democratic elections and the possibilities offered by computers. In particular, electronic voting appears to make massive and invisible fraud possible to achieve by small groups of people with the necessary skills. At present, it is not a realistic possibility to design an electronic application, remote or not, that could cope with the demands of democratic elections. Authors analysis demonstrates that traditional voting systems which use no electronic counting systems compare favourably to electronic voting systems when transparency is taken into account, transparency being a crucial factor in creating voter confidence in the voting system, and in consequence, in that of the elected representative’s legitimacy.

Simha Rahul et al. (2008) – In this paper the authors proposed end-to-end independently- verifiable voting schemes provide encrypted paper receipts to voters, who may later check that these receipts are in the electronic ballot
box. Unfortunately, few voters are likely to follow up on the voting process after leaving the voting site; as a result, few receipts will be checked. This paper describes an enhancement to E2E schemes that does not require the voter to perform a task outside the polling booth. It enables the voter to electronically transmit her receipt, from the polling booth, to a trusted external verifier. This is done through the use of a human-verifiable digital signature primitive whose (short-lived) security depends on the hardness of an AI problem. The primitive enables the voter to be certain without access to trusted computational power in the voting booth that the receipt has been securely deposited with the external verifier. The approach presents several advantages: the voter is not required to do anything outside the polling booth, no receipts are needed after polling, all receipts generated by the polling machine can be checked, and any classical digital signatures on receipts can be checked instantaneously by the trusted verifier. Additionally, an audio-based format is an easy extension for those with visual disabilities.

**Folorunso O. et al. (2010)** – The authors found some of undesirable features in e-voting as it include not allowing recounting of votes after election in case of a protest like the others. Another issue is that of erroneous software which can greatly affect the result of the election. All these is further compounded by the fact that voting systems deals with very large amount of data that is collected from a distributed population source hence the raw data are extremely difficult to comprehend and therefore monitor. This paper attempts to solve this problem using a Tree Map based visualization technique to monitor in real-time the distributed balloting and voting processes. The paper proved that Tree Map algorithms can be configured and deployed on the central server to monitor effectively the voting transactions in real-time and hence enable transparency. This work has attempted to alleviate the fear of critics of e-voting systems by adopting a form of information visualization Tree Map to monitor events in the balloting process. Though the work recognizes that there are also challenges in the adoption of visualization technologies, research has shown that this can be easily circumvented.
D. Ashok Kumar et al. (2011) – The author in his paper suggested novel design for electronic voting system using fingerprint. The accuracy and impartiality are tallied in high rate with biometric system. Among these biometric signs, fingerprint has been researched the longest period of time, and shows the most promising future in real-world applications. Because of their uniqueness and consistency over time, fingerprints have been used for identification over time. However, because of the complex distortions among the different impression of the same finger in real life, fingerprint recognition is still a challenging problem. Hence in this study, the authors are interested in designing and analysing the Electronic Voting System based on the fingerprint minutiae which is the core in current modern approach for fingerprint analysis. The new design is analysed by conducting pilot election among a class of students for selecting their representative. Various analysis predicted shows that the proposed electronic voting system resolves many issues of the current system with the help of biometric technology.

Kumar Sanjay et al. (2011) - Electronic Voting Machine is a simple electronic device used to record votes in place of ballot papers and boxes which were used earlier in conventional voting system. Being a standalone machine without any network connectivity, nobody can interfere with its programming and manipulate the result. Keeping the erratic power supply positioning 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. After the voting is completed and the close button is pressed, the machine does not accept any data or record any vote. Through the press of “total” button, the control unit can display the number of votes recorded till that time which can be cross checked with the register of voters. This paper has presented the comparative study of voting techniques in various countries which highlights the scope of improvement in them.
Ofori-Dwumfu O.G. et al (2011) - The aim of this study is to design an electronic voting system based upon the electoral process adopted in Ghana. In order to choose people to various positions different methods have been set up, with researchers continually trying to find improvement to the existing methods. The most recent method to be devised is electronic voting. It is meant to phase out outdated paper ballot, punched cards and other mechanical voting systems with paperless electronic or online voting systems. E-voting systems endeavour to make elections simple while reducing the total cost of the election. Designing an air-tight and reliable e-voting system is therefore a great task, in that, the system that must be developed must protect the privacy of the voter, be easily understood and used by the entire voting populace no matter who they are or where they come from. Based on this, OVIS, an On-line Voting System, has been developed.

Goldsmith Ben (2011) – The author had suggested in this book that the use of electronic voting and counting technologies has great potential for improving voter access to the electoral process. The author identifies a number of groups which may benefit from the greater accessibility provided by such technologies, including people with visual disabilities, those who struggle to travel to polling stations, access for those using official minority languages, military personnel overseas and citizens living and working abroad. However, using electronic voting and counting technologies also has the potential for excluding voters, especially those who may not understand how to use new systems and may feel intimidated by trying to do so. After a brief discussion on international electoral standards related to electronic voting and counting technologies, the guide will take each of these stages of the feasibility.

Howlader Jaydeep et al. (2011) - In this paper authors had presented a technique that would replace the untappable channel used in election and auction protocol by deniable encryption. The deniable encryption scheme does not require any infrastructure and easy to deploy. The prior protocols which are based on public key cryptography and assume the existence of
untappable channel are easily upgraded to a protocol without untappable channel without changing the basic encryption principle. However, deniable encryption has an expansion of the cipher size. Since, it does not use receipts and concepts of registration, so it can be effectively deployed in electronic auction mechanisms and is more secure as it does not assume untappable channels.

**Alpaslan altun Adem et al. (2011)** - In this study, an electronic voting system, E-voting for a general election is developed and fingerprint authentication based e-voting system is applied. As a result, security of the voting system is greatly improved by using biometric authentication system. Modern technology is used for elections and/or referendums commonly. Number of the reseraches on electronic election systems is increasing in recent years. As a result of being in search of more efficient, more trustable and faster election, different kinds of voting boxes are manufactured and put into service of the countries. Biometrics is also expected to be increasingly used in conjunction with other technologies like the knowledge based authentication on the Internet. In this study, user friendly electronic voting system based on biometric verification is designed and proposed. Thus, electronic voting boxes are offered instead of voting boxes of the present election system.

**Autade Kirti et al. (2012)** - This paper provides the specification and requirements for E-Voting using an Android platform. The e-voting means the voting process in election by using electronic device. We also described how the android mobile phones are efficient and can be used for voting. This paper focused on the analysis of development of E-voting application on an android platform. The usability of this system is very high if it will used in real life election process. It will definitely helpful for the users who wish to vote and the voting process will be made very easy by using this application. However, after having tested the system, in future we tend to add additional functionality of image validation for the security constraint and uniqueness which will provide very strong security for the confidential information about vote.
**Jegede A.J. et al. (2012)** - The research proposed and developed software to cater for electronic voting. Hosting the proposed electronic voting system on the Internet will facilitate online real time voter’s registration, record verification, party registration as well as the actual conduct of voting electronically via internet/telecommunication services with the resultant transparency, speed and reliability of the electioneering process. Although there may be challenges in the area of infrastructure such as electricity and shortage of personnel, it is possible for countries to adopt a gradual migration from conventional voting system to electronic voting. The gradual migration would allow a reasonable time to address the infrastructural and personnel problems as well as enable the citizens to adapt to the new approach.

**Mundalik Vijay et al. (2013)** - The target of this paper is on use techniques like Cryptography and Steganography for Password Security to Voter Account as well as by using Eigen Face recognition technique the highly more secure Online Voting System is implemented. The security level of the project can be increases by using new concept randomly generation of cover image for every user. By using Embedding and Authentication process of the system password security highly improved. Thus this technology gives chance to every citizen for voting from any place, and they can be sure that they alone can choose their Candidate.

**Aggarwal Indresh et al. (2013)** - In this paper, authors proposed to introduce a new voting system that will be accurate, transparent, and faster and will ensure a single vote for a single person. Our proposed system has covered all of these issues successfully. Moreover this system will provide boundary less voting. A better database maintenance, automated registration system and the process of casting vote using finger print will further help us to fulfil our purpose. Based on the design principles and requirement, a prototype of the system for E-voting System has been proposed by the researchers and developed. The using of electronic voting has the potential to reduce or remove unwanted human errors. In addition to its reliability, e-voting can handle multiple modalities, and provide better scalability for large elections.
Parveen Atiya et al. (2013) – The authors proposed new Electronic Voting in which a voter has to just logging on the computer with an internet connection. Also, this voting requires an access code for the e-voting through the advance report of a voter. To reduce these disadvantages, the authors suggest a process in which a voter, who has the wireless certificate issued in advance, uses its own mobile phone for an e-voting without the unique registration for a vote. In this paper, a polling scheme by means of mobile technology is resented as most fundamental application of GSM based Personal Response System, which allows a voter to cast his vote in simple and convenient way without the limit of time and location by integrating an electronic voting method with the GSM infrastructure.

Abdulhamid Shafi Muhammad et al.(2013) - After much investigation and research carried out on the manual method of voting, it was observed that a lot of problems and inconsistencies that result from the manual voting method has led to serious manipulations and rigging of the process, Electronic voting system can guarantee a credible and reliable election, with results produced in real-time and without any possibility of interference with the election results. This research work has therefore come as a platform to propose an electronic voting system that will place our democracy on a path of success. In a whole, this research seeks to increase the efficiency of voting process and the image of the independent national electoral commission. Therefore, authors recommend the followings: INEC should review the standards of ICT infrastructure in the country and develop more secure databases and networks before embarking on e-voting; there should be adoption of distributed encryption techniques for the purpose of secured data transmission; there should be use of biometric capturing devices, which will serve as a means of voter’s authentication; there should be adequate and proper public enlightenment before the system is fully implemented.

Hoque Md. Murshadul (2014) - In this paper, an Electronic Voting Machine (EVM) system is proposed which is in operation as transparent as the digital system. The Simplified Electronic Voting Machine (SEVM) responds on some
flow of pulses coming from the switch operated by voter and produces the output of the counting values i.e. total casting votes of individual nominee and displays it. The machine is controlled both automatically and manually to operate the system for successive voters and to ensure that a voter can give only one vote to his/her chosen candidate of the same position. The manual controlling system must be operated by presiding officer who have the authorization to check and to declare a voter valid after checking some unique information e.g. NID number where as the automatic controlling happens whenever a voter pushes a switch to vote.

**Sidqi Haval Mohammed (2014)** - In this paper, an electronic voting scheme using GSM mobile technology is presented. By integrating an electronic voting scheme with the GSM infrastructure, we are able to exploit existing GSM authentication mechanisms and provide enhanced voter authentication and mobility while maintaining voter privacy. In this paper, SMS has been used to send message which contain only code or identification of candidate, on the other hand used mobile to receive message and it is connected to a server to collect messages.

**Herstatt Maximilian et al. (2014)** – The author explained the social construction of the Indian EVM. The Security research team led by Hari Prasad and VeTA used the frame ‘vulnerable and risky EVM’. In many respects the electronic voting system has advantages over the paper ballot system. Yet in terms of transparency and verifiability, VeTA and the security research team claim that the paper ballot system had advantages. More radically it has been argued by them that paperless electronic voting will never be secure. This decision was decisive for closure to occur in the controversy. Yet the controversy has not only been closed in technical terms. Many of the allegations that were made about EVM malfunctions and manipulation possibilities were simply answered by neglecting them. According to VeTA and the security researchers argued that EVM has a major security flaw. Looking at the present situation of electronic voting in India fair to say that the EVM has stabilized and the controversy has been
closed, although there are still some isolated individuals who fight for their voice to be heard.

**Meher Sukanya Sagarika (2014)** – In this paper, electronic voting machine presents a way to develop a voting machine which displays the count of votes on a 16x2 LCD interface. This LCD based small scale electronic voting machine is designed for four candidates. A user can get his/her vote register through a set of switches which consists of a 3x4 keypad. The final count can be seen on LCD. The 3x4 keypad and 16x2 LCD are interfaced to microcontroller AT89C51 for various operations and displays. The author proposed the electronic voting device that is portable and the display of results are instantaneous and accurate. Appropriate message is displayed on the LCD throughout the voting process thus providing a user friendly interface. However the drawback of the device is that it is reset on power off and hence can be used only as long as it is kept powered on, thus being useful only in small scale applications. This small scale voting machine has a lot of advantages such as it is economical, less manpower required, time conscious as less time required for voting & counting, avoids invalid voting, saves transportation cost due to its compact size and convenient on the part of voter.

**Malviya Pankaj Kumar (2014)** - This paper depicts the new model of E-voting system using cloud in Indian Scenario. The preferred model is more secure and efficient than the Conventional voting system. The E-voting system avoids the delay of result it is capable to count all votes within few times. A unique AADHAAR identification number is the base point of this model. This model easily verifies to the voter and elector. In this proposed model, we have endeavoured to make more secure E-voting and it avoids unauthorized access. The model of E-voting system using cloud will enhance the transparency and reliability of the current electoral system.

**HTET NE OO et al. (2014)** - This paper presents the types of electronic voting systems as well as different methodologies for electronic voting schemes: blind signature scheme, homomorphic encryption and mixnets.
Moreover, various kinds of electronic voting systems in different countries around the world are also mentioned. This paper renders a survey on various kinds of electronic voting systems with their strength and defects. Finally, the advantages and disadvantages of electronic voting are described.

**Mythili K. et al. (2014)** - 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 SMS 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 conducting smooth, secure, tamper-resistant Elections. However these techniques will be suitable to the new technology, mobile phones like smart phones which contain android, Nokia OS. The basic model mobile phone does not support this technique. queue. In order to improve the voting ratio SMS voting has been introduced. This article discusses complete review about voting devices, Issues and comparison among the voting methods and technology support for SMS voting.

**Pedgulwar Ashish et al. (2015)** – The aim of the author in this paper is to provide the details and need for e-voting based on android system. In election electronic device is used for voting process i.e. E-voting. The e-voting uses SMS protocol. In this proposed system we are providing e-voting system through SMS using Smartphone so result shows that there is no need of internet in their mobile. In Smartphone there will be an android application through which voting process will be done without internet in Smartphone. A real-time e-voting system based on android phones. The analysis of this system is based on SMS voting. It is then developed by implementing techniques using android platform. If this system will be used in real life election process then the usability of this system is very high. It will definitely helpful for the users who wish to vote and the voting process will be made very easy by using this application.
Nithya Ms. J. et al. (2015) - By application of this project into real time we can avoid malfunctions, Time maintenance system, Automatic counting of votes. It is also insensitive to variations in the lighting conditions and noise levels. It specifically uses the zero crossings of the wavelet transform of the unique features obtained from the grey-level profiles of the iris. It uses only a few selected intermediate resolution levels for matching, thus making it computationally efficient and less sensitive to noise and quantization errors. Iris detection in the application works to a very high degree of accuracy in every seen case. This, unfortunately, is not a property shared by the iris, making it significantly more difficult to isolate than the pupil. Day by day the population is increasing enormously which in turns demands the improvement in the voting system. The primary goal of every voting system is to increase the participation of the civic. Undoubtedly the above discussed voting techniques are exceptionally good, but there is always scope for further improvement.

Pandit Anil et al (2015) - This paper focuses on various security flaws in the design of EVM hardware for voters and voting protocols that support the voting process, without implementing the security mechanisms required for preventing fraud and protecting voter's privacy. Slew of security concerns have been raised and various references have been added in this paper to support our issue of security in EVMs'. This paper describes the overall security issues in the hardware of EVMs microprocessor of the EVMs', the EVM's firmware is stored in masked read-only memory inside the microcontroller chips, and there is no provision for extracting it or verifying its integrity. The main objective of this paper is to describe the primary role of E-Voting and its security in securing the voters privacy, verifiability, coercion and accountability by implementing cryptographic algorithms while transmitting Electoral Voting Data in a Centralized Pool. In this paper the authors have analyzed issues of security in EVM used in many countries in their election process. Strong demerits were reported in our paper regarding the hardware and functioning of EVMs Traditional authentication and authorization mechanisms cannot fully cover the security requirements of the administrative workflow in EVM. An extension of the authentication-
authorization scheme is necessary only when cryptographic mechanism is put in place.

Lauer Thomas W. (2015) - This paper considers two different e-voting schemes, Internet voting and direct recording electronic (DRE) voting systems, explicitly focusing on risk to the integrity of the voting process. Fair elections must assure voter authentication, vote confidentiality and integrity, and the ability to audit the election. E-voting poses special challenges. The paper analyzes security risks that may threaten e-voting schemes and makes recommendations. There is strong indication that the deployment of e-voting systems will continue. This should not be done at the expense of conducting fair elections. This analysis has shown where of the risks lie.