Available at: www.researchpublications.org

Design of E-election System

Dr. Vinod. M. Patil
Head, Associate Professor
Department of Computer Science,
Shri Shivaji College, Akola
Akola-444001, MS, India
e-mail: vinmpatil2@yahoo.co.in

Abstract*: In aspect of designing the electronic voting system, force to consideration of different subject such as software engineering and hardware engineering, cryptography, politics, law (legal), economics and social sciences and the various requirements. The most important fact that concerning to the similarity to the procedure of traditional voting system and electronic voting system in order to easy operate by voter and manage by poll workers. That is the main problem face by designer of the e-election system and administrator and voters.*

Keywords: Secrete key, Private key , key encryption, privacy, voter ,poll worker etc.

I. INTRODUCTION

Electronic balloting and voting can make the election process more convenient and efficient if it can be achieved securely as well as preserve the voter's privacy. The basic principles of democracy are base on collective decision making of citizens through the voting process. It may be consider as an important indicator of democratic process. The principle of pole of civilization through voting process is a society decision-making results and which is the basis of the paradigm. Assuming that the ultimate democratic process would provide the facility for all citizens to vote on all decisions. The purpose here is to show how the use of Information Technology play an important role for a new step towards democratic process. Not only it changes the scale of decision making but also it permits creation of new communication links and decision making process that do not exist earlier in the political structures. Here try to achieved practically the two things simultaneously that are voter's privacy against security.

In order to preserve the voter's privacy, require to generate pseudonyms for each voters that cannot directly link to the voters registration or identity. Also cannot identify the voters by the election authority or any political party or anything else without the permission of voter and other three groups form for the purpose of privacy. The group means consider the different groups related to the political party, related to the NGO or social groups or any individual verification and related to the election authority itself.

II. DESIGN ASPECTS:

The issues of design of electronic voting system are concerned with the requirements of appropriate algorithms and mechanisms to easier the voting process. The effective action of an e-voting system is unavoidably associated with a distributed system, which force to introduces security and privacy of the voters. This requires the design of a specific voting protocol, maintaining of electronic data , implementation of process and integration of relevant mechanisms.

The following critical conditions are required to construct the design of e-voting system.

- Secure communication channels to ensure privacy and secrecy.
- Anonymous channels to prevent the linking of a specific vote that was cast by the voters.
- Remarkable line of separation between the related fields and the discharge of functions by reliable and trustworthy agencies.
- Convenient and secure interfacing mode and data storage.
- Quick availability of voters data and records without disturbance.

In e-voting system a communication channel must be secured if it ensures secrecy through the use of symmetric or asymmetric key encryption; and ensures data integrity by means of digital signatures, message digests or message authentication codes (MACs).

III. THE MAIN CHALLENGES OF DESIGNING ELECTRONIC VOTING SYSTEM:

The main challenges of electronic voting system that are to be faced during designing, developing and maintaining [1] are as follows:

- **Sources utilization:** The Various available electronic equipment (sources) and documents relating to EVS provide high-level principles and recommendations for e-voting machines. However, when transferring and managing the election from paper-based to electronic. This type of information has to comply with acts for regulating elections as an electronic election. The actual requirements from these principles regarding integrating and maintaining traceability of machine becomes an important aspect to guarantee that an effective management of these sources.(e.g. when in India, election commission had to start the bye-election by using the EVM in south Kerala constituency in 1882 high court struck down the process on the ground that EVM process has not legal aspect according to the law.)
- **Decrease the gap of design and requirements aspects:** When the election process has been carried out by using electronic voting system, an approach strongly inspired by the spiral development process, to speed up the development with electoral events. However, this requirements should be define in a simple and clear strategy in order to manage

electronic system across the different phases of the process and across the country and thus, to help to reduce the gap between requirements and architecture of the system.

- **Flexibility of Software :** During the implementation of electronic voting system in different election (e.g., municipality, assembly, parliament , councils, and unions representatives) the corresponding software requires to be so flexible that can easily be configured for variation in ballot , voting options, counting algorithms (as per the preferential voting system) etc. The use of the system for different elections increases the complexity of managing configurations and recognizing logical sections which allow the program to be modularized.
- **Hardware Requirements and configuration:** During the use of electronic voting system, different electoral events and different electoral offices require hardware and configuration of the hardware system. On the ground of that, the natural evolution of the system made us to experiment basis that introduce a new hardware components (such as, PC, BIOS, external LCD display, Printers). Requirements had made so simple that can, allow a flexible management to configuration, the hardware for the specific requirements of the election system.
- **Compatibility of EVS with the traditional electoral procedures:** An important factor concern here, are the legal and usability concern to the compatibility of electronic voting system with the current electoral laws and processes. In general, in order to provide a smooth functioning after conversion from traditional paper-based voting to e-voting system. As the voter's point of view, the process should be as similar as possible to the manual one and poll workers should be able to recognize procedural steps by step as they are familiar with previous one.

IV. THE MAIN FEATURES OF THE SYSTEM:

Described here the main features of the electronic voting system that is proposed by using OLAP algorithms:

- ➢ The system fulfils all most all requirements, condition and legal aspect that need to implements the EVM.
- ➢ Ensure that system provide the excellent security by using OLAP algorithm for all the interactions among different module of the system.
- ➢ No one can falsify the result of the e-voting process because the votes are verify by every other module of the system.
- ➢ Voters can easily check whether their votes are counted correctly in a final tally or not, in other words, citizens can verify their votes individually or universally of course without compromising their privacy.
- ➢ No other citizen / person can know to whom the voter voted for except himself / herself, i.e. Ballot is kept confidential / secret / unknowns to the outsiders and even administrators.
- ➢ System provides a very simple interface that is easy to operate and configure the hardware and software as per the requirements of local, regional and national assembly election and bye elections.
- ➢ System provides automatic generation of the ballots / options through easy to use interface and configuration by the concern election authority.
- ➢ System provides the provision of easy online registration system, once the identification and recognition of voter by the election authority.
- ➢ Only eligible voters can vote only once by using our system, since registration is only allowed to them through private and public key with identification number.

A. ASSUMPTIONS:

Assumptions for the e-voting system**:**

- An inexpensive, easy-to-use read / writes electronic storage medium is available.
- A hardware device accompanying with software is capable of reading and / or writing (recording) to the available storage media that will reliably record / updates the same information locally or on the server or in the external public Bulletin board at a time to avoid the discrepancy.
- Polling booths are completely enclosed. i.e. contain inside the building and all entrance and exit are watched since nobody can vote forcefully or by using economic power in favors of it after voter get identified by voting registration card.
- Provide the voting machine such that the voters can physically capable of operating it. e.g. touch screen computer equipment and / or standard PH SCI [2] hardware such as keyboard mouse, monitor, mouse etc. and of holding and moving registration cards.

The main process is listed below:

a) **Pre election**

- Election
- Candidates
  - Nomination
  - Response to nomination
  - Candidate List
- Voters
  - Voter registration
  - Inter database communication
  - Voter List Preparation
  - Voter duplication removal
  - Polling information
  - Voter Notification

b) **Election**

- Voting
  - Ballot
  - Authentication
  - Verification Reply
  - Vote Confirmation
  - Votes

c) **Post election**

- Counting
  - Count Result
- Audit
- Analysis
- Declaration of results

d) **Global functions**

- Administration Interface

- Help Desk

B. Ballot:

The term ballot is used to denote the message which is issued by election authority to the voter in order to cast a vote for a specific candidate. e.g. the ballot is an encryption of the vote, while the vote reads as “Candidate X”. Thus, the ballot is nothing but an envelope that containing the actual vote of the voters.

C. Data:

During the election processes the different kinds of data require their content as well as structure are to be defined as follows:

- The electronic ballot signed by a voting authority to make it valid.
- The digital certificates which allow proving identities and encoding data in order to make it readable only for election authority. However, there are many incompatible standards for digital certificates, e.g. X.509, SPKI, and Open PGP. If biometric data is used for identification one has to define how fingerprints, facial recognition data, or/and iris scan data are stored.
- The vote’s ballot must be stored.
- A major problem is vote receipts. If used, then they should violate the voter’s privacy.

D. Functions:

The functions are required in the algorithms such as algorithms for encoding and decoding (including key length), signature algorithms as well as algorithms for blind signatures and anonymous channels. If possible, to applicable, precise biometric identification algorithms must be applied.

E. Authorities:

In the election process, the different election authorities have been involved to execute the election. Numbers of authorities have been proposed for making a ballot secure. The question is that which authorities are responsible and even protections precautions regarding rooms, servers, etc. are to be specified.

F. Hardware and Software:

As regarding the security of both hardware and software are important, relating to the voter’s PC at home think about malfunctioning software (viruses, worms, Trojan horses, etc.) that could change, delete or read the voting decision unnoticed. A solution might be external devices like smart card readers with a keyboard and/or display that work as an interface to smart cards (with own memory and microprocessor). Approved or certified software can be stored on the smart card which is responsible for secure encoding and signing. Moreover on all computers only approved or certified software should be applied.

G. Organization:

The basic requirement of electronic voting systems are the (static) infrastructure and the (dynamic) protocol included as organization, as they integrate and combine all other elements. The protocol determines the voting process and the infrastructure determines devices and software reside (e.g. how many voting servers exist, level of redundancy) and in which way they are linked to each other including technical protocols. On the other side the most challenging security requirements is protection against DOS (denial of service) attacks. Only if each element accomplishes specified security requirements then can get a secure voting system.

The function of each section within the database is described below.

- **Voter**: includes all voter’s data for every voter such as ID, password, private key etc.
- **Candidates:** includes all contesting candidates.
- **City:** includes all cities / villages and binds every city / village to its district.
- **Confession:** includes all confessions in the country.
- **Constituency:** includes all constituencies in India. The particular area or region as per the type of elections (assembly / parliament / local).
- **Election Cycle**: includes the election cycles or phases of election inorder to complete the process.
- **Election Type**: includes the type of elections: Legislative or Municipal or assembly or parliaments or local etc.
- **Governorate**: includes central and all state governments in the country.
- **Nominating**: includes all candidates that are interested to contests the election for a given election. The number of votes cast for each candidate is increased according to voters' ballot. The **Constituency_Id** field designates the **Seat_Id** or the **Division_Id** for the legislative or local elections respectively.
- **Polling center**: includes all polling centers / polling booth in country and binds every polling center to its circle / division.
- **Division**: includes all division / circle in country and binds every city / town to its corresponding division / circle.
- **Seat**: includes all Parliament / assembly seats distribution and binds every seat to its district and its division/ circle.
- **Voters Ballot**: includes all choice to voters and list of all candidates that are participating in the election. The voters' ballot is not saved in order to maintain confidentiality.

V. ARCHITECTURE OF E-ELECTION SYSTEM:

The architecture of proposed E-election system is comprised of four components:

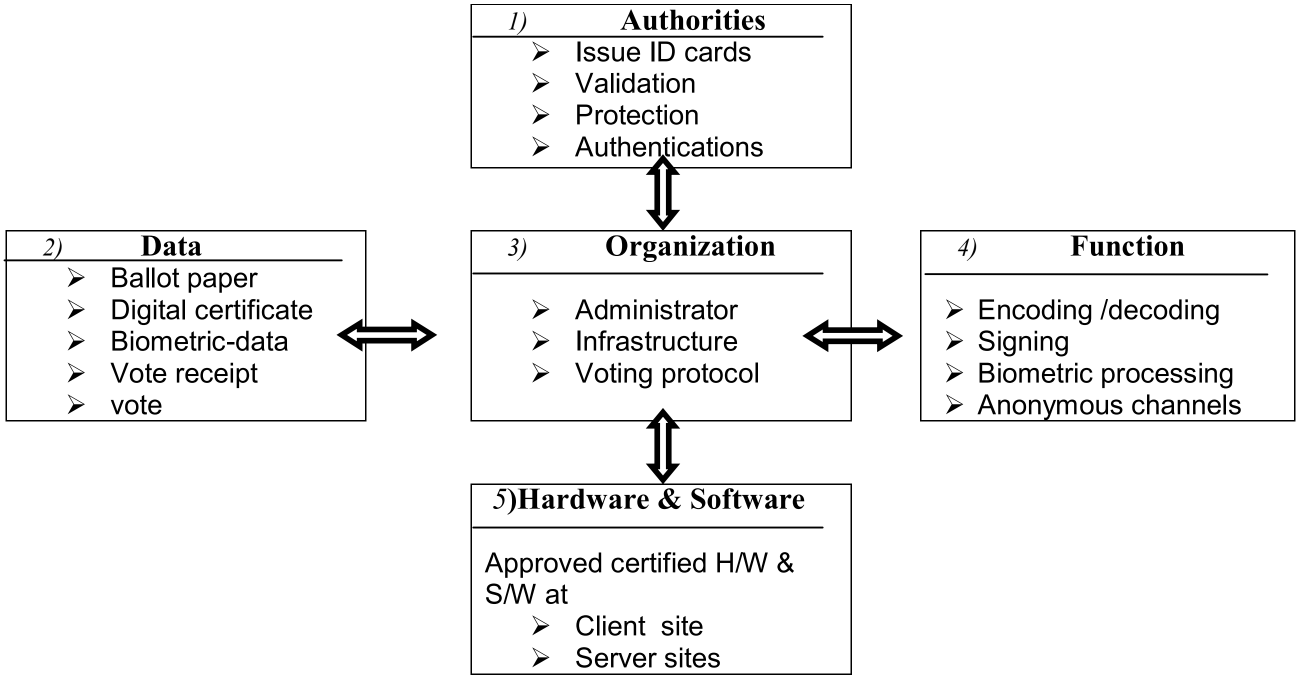
a) Multipurpose card / Smart card / other Identification card for each eligible citizen who may vote for election process;

b) Terminal that capable of reading the card/ recognize the voter after identification and communication on both sides with the voters and validator;

c) An access to internet / Intranet;

d) Server that is capable to collect and manage the huge amount of data (votes);

It will be implemented through fully Computerized Internet network. It includes following methodology: Some of the following steps will be carried out on experimental Simulation.



- ISP to launch election portal with database driven web site.
- Central Server with high capacity.
- Web server to each taluka level place.
- Strong communication link.
- Computer voting machine (Terminal) to every polling booth.
- Computer nodes to every election office.
- Video conferencing facility to polling booths.
- E-elections portal with all databases and bulletin board (BB).
- E- elections control and management software.

FIGURE 1: FRAMEWORK FOR ELECTRONIC VOTING SYSTEMS

VI. RELATIONAL DATABASE OF E-ELECTION SYSTEM:

Figure shows the Relational Model of the system database. The Relational Model satisfies all the needed features as per the requirements.

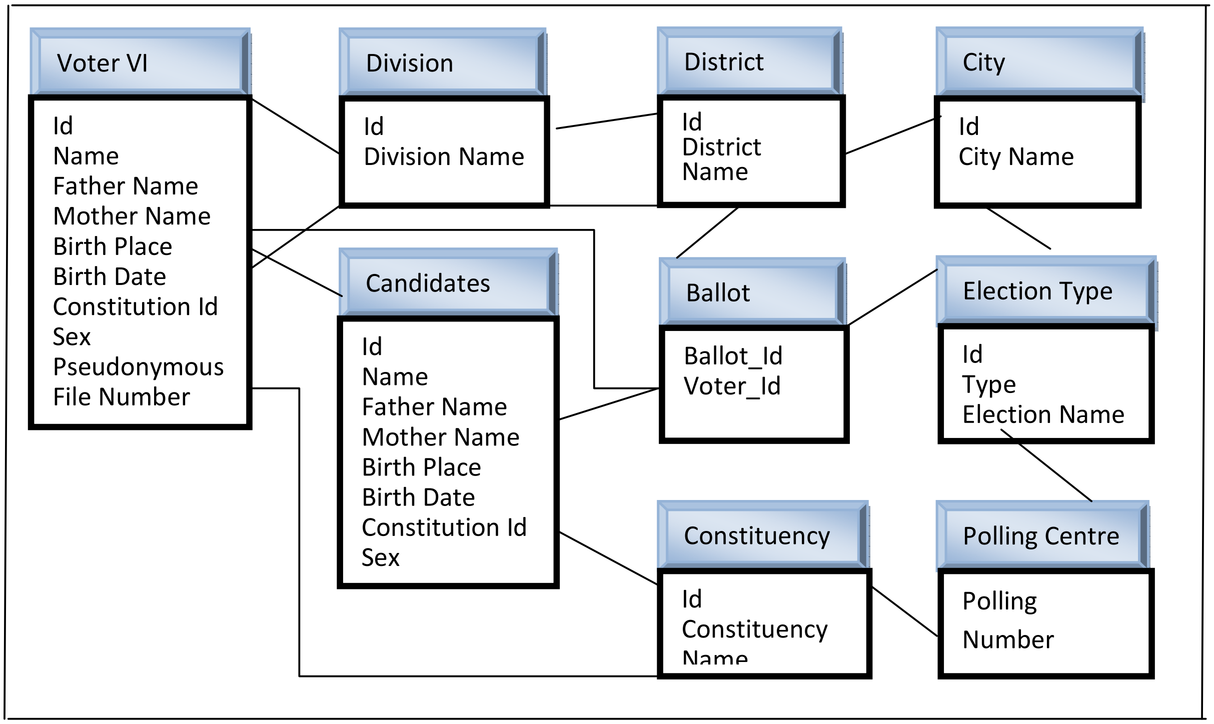


FIGURE 2: GENERAL SCHEMATIC DIAGRAM OF PROPOSED SYSTEM ARCHITECTURE

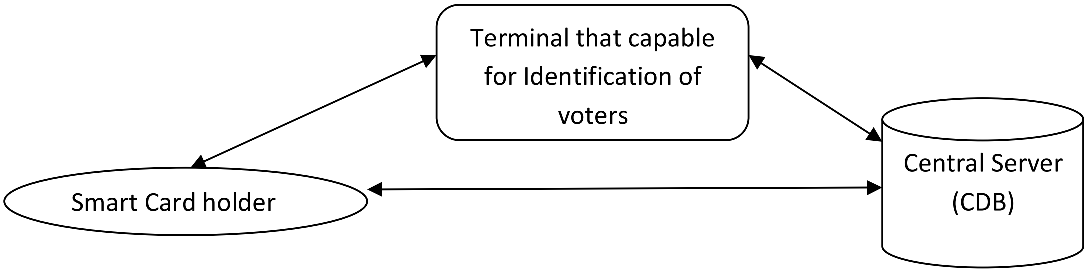


FIGURE 3: GENERAL SCHEMATIC DIAGRAM OF PROPOSED SYSTEM ARCHITECTURE

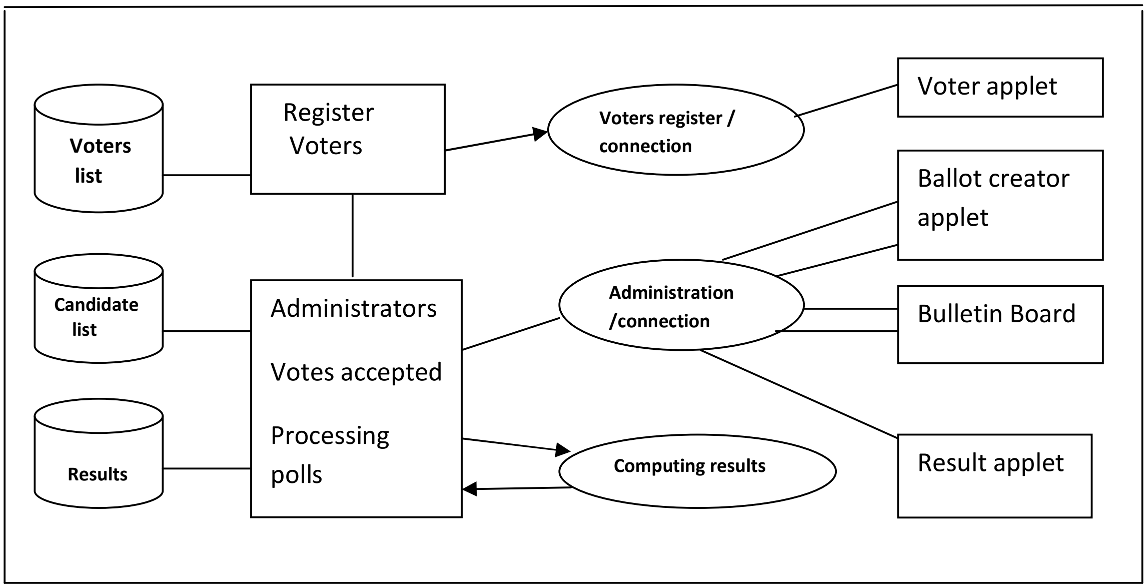


FIGURE 4 : SERVER ARCHITECTURE

VII. Working of the Algorithms:

The following steps are needed for the working of the proposed Algorithms:

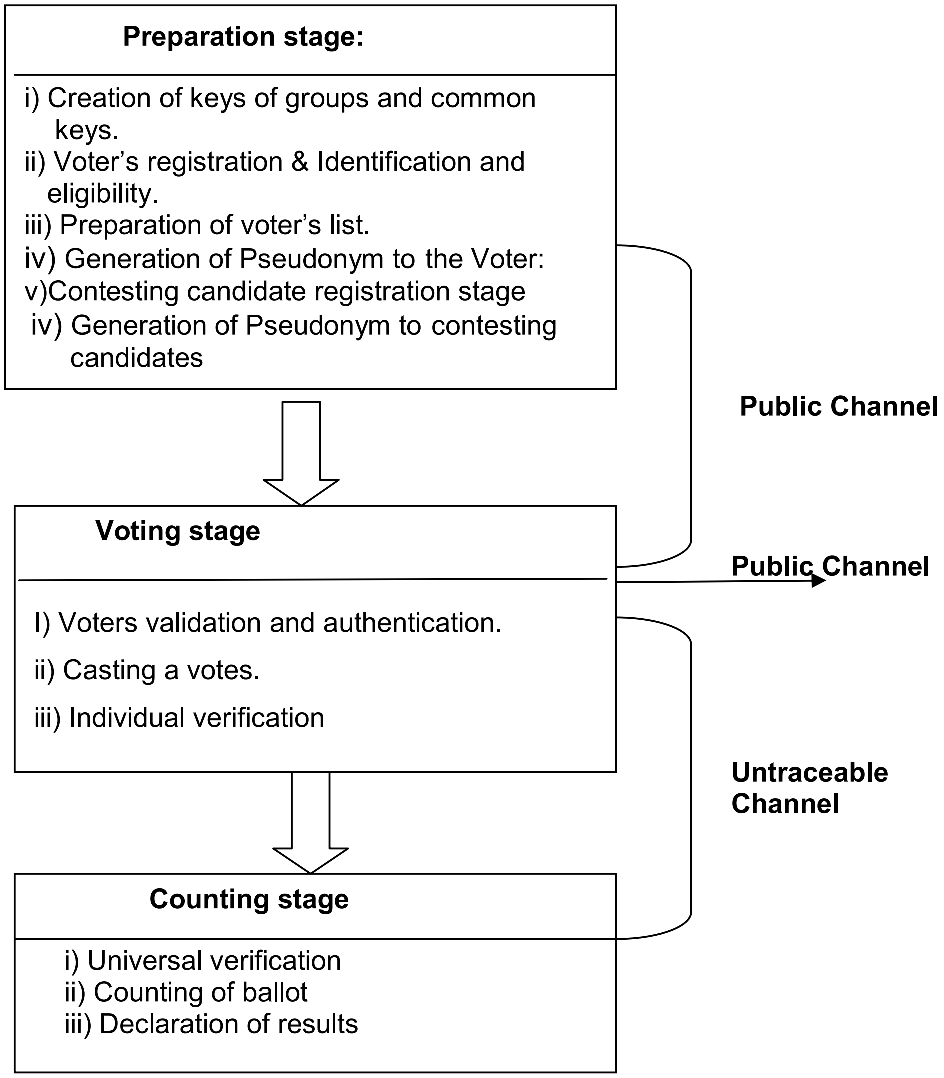

Preparation stage:
i) Creation of keys of groups and common keys.
ii) Voter's registration & Identification and eligibility.
iii) Preparation of voter's list.
iv) Generation of Pseudonym to the Voter:
v)Contesting candidate registration stage
iv) Generation of Pseudonym to contesting candidates
Public Channel
Voting stage
Public Channel
I) Voters validation and authentication.
ii) Casting a votes.
iii) Individual verification
Untraceable Channel
Counting stage
i) Universal verification
ii) Counting of ballot
iii) Declaration of results

FIGURE 5: VOTING PROCESS FLOW-CHART

VIII. THE ROLE AND ARCHITECTURE OF THE SERVER:

The first role of the server is to replace the voting complexity. Then functionally it has to:

- Verify the identity of the voter and candidates
- Available the voting Information (Data);
- Receive the valid vote only
- Collect and aggregate the votes in the respective heads and count in a final result or communicate to the bulletin board.

For the privacy of voters, pseudonyms are used instead of personal ID and the tracing of the votes from the public network is protected by the assumption of the existence of anonymous communication channel. When voters in the system want to begin communication, the client (voters) firstly gets the server's public key published bulletin board in initialization stage. Then terminal generates a secrete key, encrypts it with the public key, and sends it to the server. When the server receives it, he decrypts it with his private key. Now the server and the voter can begin to communicate each other

a. Administrator:

1. Create and Retrieves the voters list;
2. Create and Retrieves the contesting candidates list
3. Sends to each voter a copy of the Validator public key Y_i (used for the encryption of validation requests by the voters),
4. Sends to each voter a copy of the candidate list from which the voter makes his / her choice.

b. Validator:

1. Generates a public / private key pair to each voter V_i.
2. Generates a public / private key pair to each candidate C_j.
3. Receives validation requests from voters V_i.
4. Checks that the voter is eligible and that the voting code Id is correct,

4.If code Id is valid, signs SG_i to the vote and returns it to the voter V_i.

c. Collector:

1. Receives encrypted votes from voters and store it in centre database CDB.
2. Strips off Id and any identifying information (communication headers etc.) and stores the votes V_i in their encrypted format PV_i until the election is complete.
3. Collect the votes of the respective candidates and forwards them to the Counter.

d. Counter:

1. Decrypts the votes choice for corresponding contesting candidates arrays
2. Verifies that the Validator has signed SG_i for each voter V_i.
3. Tallies the voters Votes.
4. Publishes the list of public key Y_i and corresponding vote values in the bulletin board.
5. Publishes the results in bulletin boards BB.

e. Key Server:

1. Collects public keys from group A, group B, group C and the Validator and Counter,

2. Distributes the keys to the servers.

IX . CONCLUSION:

In order to maintain the democratic environment in the nation the election process is play an important role. To achieve this it is necessary to develop a system for voters electronically in a secure and secreate manner by using electronic voting system (e-election). This lead to find a way to do the guarantee to fulfill all the requirements with a relative high degree of security and accuracy against the preserving the privacy of the voters. The design of electronic voting system is a task of covering all aspect that fulfill the necessary requirements along with traditional election process and accepted by all political party, social ornanization, election commission , faith by voters and government. This design of election process not useful for verification at every stage of election process but also useful after the elections.

X. RERENCES:

[1]. Weldemariam, K.; Mattioli, A.; Villafiorita, A.; “Managing Requirements for E-Voting Systems: Issues and Approaches”, First IEEE International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 Page(s): 29 – 37.

[2]. Xiangdong Li, Michael Carlisle, Andis C. Kwan, Lin Leung, Amara Enemuo and Michael Anshel, “An Elementary Electronic Voting Protocol Using RFID”, Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY 20-22 l-4244-1304-4/07, 2007 IEEEJune 2007, pp 234-238.

[3]. Antonyan, T.; Davtyan, S.; Kentros, S.; Kiayias, A.; Michel, L.; Nicolaou, N.;Russell, A.; Shvartsman, A.A.; “State-Wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity “ , Information Forensics and Security, IEEE Journals , Transactions on Volume: 4 , Issue: 4 , Part: 1, Page(s): 597 – 610.

[4]. Fauzia, N.; Dey, T.; Bhuiyan, I.; Rahman,M.S.;"An efficient implementation of electronic election system ", IEEE, 10th international conference on Computer and information technology, 2007. ICCIT- 2007, Page(s): 1 – 6.

[5]. Weldemariam, K.; Villafiorita, A.; Mattioli, A.; "Experiments and data analysis of electronic voting system" , Fourth IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS), 2009, Page(s): 105 – 112.

[6]. Seo-Il Kang and Im-Yeong Lee, "A Study on the Electronic Voting System using blind Signature for Anonymity", Hybrid Information Technology, 2006. ICHIT'06. Vol 2. International Conference on Volume 2, Nov. 2006 Page(s): 660 – 663.

[7]. Athanassios Kosmopoulos ,"Aspects of regulatory and legal implementations on e-Voting ",s. wang et al.(Eds):ER workshop 2004. LNCS 3289, pp. 589-600, 2004.

[8]. J W Bryans, B Littlewood, P Y A Ryan, L Strigini, " E-voting: Dependability Requirements and Design for Dependability", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on 20-22 April 2006 Page(s):8 pp.

[9]. Kiayias, A.; Korman, M.; Walluck, D.; "An Internet Voting System Supporting User Privacy", Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual Dec. 2006 Page(s):165 – 174.

[10]. Anthony Watson, Vincent Cordonnier , "Information Technology Improves Most of the Democratic Voting Processes " Professor, Edith Cowan University - Perth, Australia , Professor, UniversitC des Sciences et Technologies de Lille – France , 1529-4188/01, 2001 IEEE ,page 388-393.

[11]. Jared Karro and Jie Wang "Towards a Practical, Secure, and Very Large Scale Online Election", Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual 6-10 Dec. 1999 Page(s):161 – 169.

[12]. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, "Analysis of an Electronic Voting System", Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on 9-12 May 2004 Page(s):27 – 40.

[13]. Lorrie Faith Cranor, Ron K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet", Public Policy Research AT&T Labs Research, 1060-3425197, 1997 IEEE, pp 561-570.

[14]. Alam, M.R.; Masum, M.; Rahman, M.; Rahman, A.; "Design and implementation of microprocessor based electronic voting system", IEEE 11th International Conference on Computer and Information Technology, 2008. ICCIT 2008, Page(s): 264 – 269.

[15]. Cottin, N.; Mignot, B.; Wack, M., "Authentication and enterprise secured data storage", Emerging Technologies and Factory Automation, 2001. Proceedings. 2001 8th IEEE International Conference on Volume 2, 15-18 Oct. 2001, pp 245 – 252.

[16]. Chai Wah Wu, "Multimedia "On the design of content-based multimedia authentication systems", 10.1109/TMM.2002.802018, IEEE Transactions on Volume 4, Issue 3, Sept. 2002 pp 385 – 393.

[17]. Won Jay Song; Byung Ha Ahn ,"Secure transmission of the prescription order communication system based on the internet and the public-key infrastructure using master smart cards in the 2-way type terminal ", System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on 7-10 Jan 2002 IEEE CNF pp :2035 - 2042.