ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

TECHNICAL NOTE

Available Online at www.ijarcs.info

Towards Individuals and Universal Verification of On Line Election System

Vinod. M. Patil
Head Department of Computer Science,
Shri Shivaji College, Akola-444001,, MS, India
vinmpatil2@yahoo.co.in

Abstract: Formation of a democratic government depends upon the faith on an election system that conducted by election authority play an important role. Inorder to increase the faith on government the verification of election process are the essential part of the system. When the voters casted their votes have been recorded correctly as per their intention and accounted in the final tally and there should be reliable and demonstrably authentic election records. To prove this process the verification are essential part. Verification process include to verity the transaction in full confidence at any time or at the time of voting. A receipt of our transaction is required that provides full confidence, at the time of voting, that our choice were accurately recorded. Election authority must provide a record that voters vote are recorded as per intention.
Voters can be sure that their votes are tabulated correctly, but voters are not required to verify their votes, in order to ensure election integrity. It is the provability that the final tally is correct.

Keywords: Private keys, Public keys, Individual and universal verifiability

I. INTRODUCTION

Election, voting etc. are well known terms in modern days of Democracy. Elections are at the heart of the democratic form of government and voting is usually recognized as one of the main characteristics of democracy. However there are need to providing sufficient protection, security and faith to stand them and hence it is critical to the proper functioning of a democracy. A general election process is an enormously complicated process involving elaborated distributed coordination of personnel, procedures, and equipments. The problem of ensuring integrity is one that must necessarily involve such disparate issues as equipment custody, voting day procedures, election official selection and training, voter training, tabulation procedures, and finally faithful behavior on the part of the actual physical apparatus [1].

II. E-ELECTION SYSTEMS

Electronic election is a very recent idea regarding voting. Electronic election, as the name implies, is the election process held over electronic media, i.e. computers. Electronic voting (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 carrying (through computer Networking media) as well as counting of votes.

Regarding the computerization of election process from start to finish, there are many problems to face such as legal and technical problem that must be solved in order to complete the process. The election process consists of several stages such as registration of eligible voter, casting of votes, counting of votes and after verification displaying of results. To design an efficient algorithm, there are many difficulties those must be overcome [2].

III. VERIFIABILITY

The security requirements of individual and universal verifiability are legally motivated by the principle of the public nature of elections [3]. For that purpose, assume the existence of a public bulletin board that can open publically, as this is a fundamental means to ensure individual and universal verifiability in electronic voting system.

A citizen opinion is that, an e-voting system must be verifiable by voters and any one that doubt about the function and working of voting system whether casting and counting ballots are performed correctly or not. Therefore, verifiable e-voting system should perform the following two distinct checks:

a. ***Individual-verifiability:*** Any voter can check individually whether her / his votes are recorded correctly as per the intention.

b. ***Universal-verifiability:*** Anyone can check universally whether the recorded all votes are counted correctly that is public audits.

A. Individual verifiability:

Individually each voter can verify that his / her vote is recorded in the final tally. Here distinguish inner and outer individual verifiability, depending on whether the voter can verify that his ballot contains the vote as per intended to cast. The expression "intention" - presupposes that the voter managed to enter his choice correctly at the voting terminal [4].

a. **Inner individual verifiability:** The voter can verify that his ballot has been published on the bulletin board, and that the ballot contains the vote that the voter intended to cast.

b. **Outer individual verifiability:** The voter can verify that his ballot has been published on the bulletin board, but cannot verify that his ballot contains the vote which the voter intended to cast.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

Inner individual verifiability allows each voter to verify that his vote has not been deleted or altered, i.e. that the integrity of the individual vote has been preserved. With outer individual verifiability the voter cannot be sure that the vote contained in his ballot has not been tampered with

B. Universal Verifiability:

Universal verifiability means to verify publically that all the votes recorded correctly in the final tally as per the intention of voters. Here it is distinguished into continuous and discrete universal verifiability depending on whether verifiability applies to all or just to a subset of steps in the processing of the ballots.

a. ***Continuous universal verifiability****:* Any interested party can continuously verify whether the processing of the ballots is correct, including all steps that were taken starting from casting of votes up to the tally computed in the last step of the election.
b. ***Discrete universal verifiability****:* Any interested party can verify a certain parts of the processing of the ballots whether it is processing correctly. However, there is no continuous verifiability which comprises all steps that were taken from starting of casting of votes to the final tally computed in the last step of the election system.

Continuous universal verifiability ensure that casted vote was not deleted, altered, invalidated or duplicated during all steps that were taken by the voting system from the votes cast to the votes tallied. Thus, the continuous integrity of the collection of ballots which have been cast can be verified [5].

While discrete universal verifiability refers to single components of the voting system and verifying these steps processed to the collection of ballots in a way that preserved the integrity of the contained votes.

IV. ASSUMPTION AND NOTIFICATIONS:

The following notations are use in the algorithms in order to develop the equation.

A. Voter's notation used in the algorithms:

Vi – Voter, Vi Є V
V - The registered list of Voter Vi and i = 1,2,……,n;
Xi - Private key of voter Vi and Xi Є X
X - The list of private key and , i = 1,2,……,n;
Yi - Public key of voter Vi and Yi Є Y
Y - is the list of public key and , i = 1,2,……,n;
PVi - Pseudonyms of the voters Vi Є V
PV - The list of Pseudonyms of the voter and , i = 1,2,……,n;
Bm - Bio-metric information of voter Vi
SGi - System signature of voter Vi.

B. Contesting candidates notation used in algorithms:

C - List of contesting candidates.
Ci - Contesting Candidate i , Ci Є C and i = 1,2,……,m;
Si - is the Secrete key of contesting candidates Ci Є C.
Ri - is the Public key of the contesting candidates Ci Є C.
PCi - Pseudonym of the contesting candidate i and PCi Є PC. Where i = 1,2,……,m;
PC - List of pseudonym of the contesting candidates.

c) Voter Ballot notation used in algorithms:

Yi = Bi - Ballot of voter Vi, Vi Є V
Bb - Blinded ballot of voter
Bbsv - Blinded ballot sign by voter
Br - Register ballot i.e. Ballot sign by election authority (i.e. Bbsv sign by election authority)

d) General notation used in the algorithms:

P - A large Prime number which is computationally impossible in the discrete logarithm.
G – Generator of prime number P.
CDB - A Central Database of the voter.
LDB - A local Database of the voter.
BB - Electronic Bulletin Board to publish any information related to election.

V. INDIVIDUAL VERIFICATION BY THE VOTER

Thus the every voter Vi can easily can check individually his / her votes are included correctly in the final tally or not. This can be check by using the public key Yi and his / her choice code ECi from the bulletin board BB. Since the public key Yi is unique key throughout the Nation and choice code is nothing but the multiplication of PVi * PCj and both are not also the actual numbers they are the pseudonymous of voter Vi and contesting candidates Cj. They are also encrypted by the common key of CKi which can be form by the permission of three groups A, B and C and the voter by combination of Xi , Xa, Xb and Xc. Hence there is no any chance of decryption of the choice code. Even through if any one try to decrypted, then still there is no chance of identification because this is also a product of two pseudonymous of voters and candidates. That is also require the conversion of PVi and PCj from pseudonymous to actual voter and candidates and this is impossible due to requirements of secrete keys and public keys.

This can be numerically verified as follows:

Since the bulletin boards are published only the two codes (Yi, ECi) where Yi is the ballot number of the voter Vi along with the encrypted code of the voters choice ECi that can show the to link of the voters choice to the selected contesting candidates which will be help to prove the requested choice was recorded by the voting centre and calculated in the final tally.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

VI. NUMERICALLY PROVE THIS AS FOLLOWS

The encrypted product of the Pseudonymous voters and candidates ECi is as under.

ECi = ECKi (PCj * PVi)

Decrypt this product to get PCi * PVi as follows:

PCj * PVi = DCKi (ECKi (PCj * PVi))

And separate the candidates Pseudonymous.

PCj = (PCj * PVi) / PVi

Table 1 : decryption of product of pseudonymous voters and candidates and separation of pseudonymous candidates.

Voters Vi	Voters Private key Y_i	$EC_i = E_{CKi}(PV_i * PC_j)$	$PV_i * PC_j = D_{CKi}(E_{CKi}(PC_j * PV_i))$	Pseudony-mous of candidates Pcj
V1	11.63985497	26441787.07	104701.8251	8995.114235
V2	11.66982947	35476421.16	131000.5854	11225.57838
V3	11.69988117	83357401.42	288207.5731	24633.3761
V4	11.73001025	90219817.6	293119.1421	24988.82234
V5	11.76021692	37479564.82	114788.9708	9760.786865
V6	11.79050137	17087540.59	49475.11023	4196.183746
V7	11.82086382	110889575.8	304309.1155	25743.39069
V8	11.85130445	121045896.4	315574.1215	26627.79636
V9	11.88182347	1321982.286	3281.125956	276.1466675
V10	11.91242109	21695405.54	51363.01444	4311.719177
V11	11.94309749	51784269.43	117148.3081	9808.87146
V12	11.9738529	145656991.7	315379.6352	26339.02704
V13	12.0046875	35011373.27	72665.79929	6053.118774
V14	12.03560151	175439336.5	349520.5144	29040.55225
V15	12.06659513	185132678.8	354500.3061	29378.65259
V16	12.09766856	84917593.28	156474.432	12934.26343
V17	12.12882201	149829149.4	265976.7517	21929.31445
V18	12.16005568	153984530.6	263623.4759	21679.46289
V19	12.19136979	203733244.9	336711.4658	27618.83789
V20	12.22276453	85583031	136670.9066	11181.66895
V21	12.25424012	123905855.8	191360.5144	15615.86133
V22	12.28579677	73929785.08	110512.1454	8995.114235
V23	12.31743468	95492722.82	138270.3284	11225.57838
V24	12.34915406	216727733.4	304201.3565	24633.3761
V25	12.38095513	227228295.9	309385.4881	24988.82234
V26	12.41283808	91672729.07	121159.0669	9760.786865
V27	12.44480315	40679497.68	52220.68069	4196.183746
V28	12.47685052	257450055	321196.4375	25743.39069
V29	12.50898043	274549993.2	333086.5834	26627.79636
V30	12.54119307	2933927.284	3463.208673	276.1466675
V31	12.57348867	47180056.77	54213.35221	4311.719177
V32	12.60586743	110486867.5	123649.3333	9808.87146
V33	12.63832957	305259748.2	332881.3044	26339.02704
V34	12.67087531	72149043.22	76698.31324	6053.118774
V35	12.70350486	355835637.7	368916.7966	29040.55225
V36	12.73621844	369903982.4	374172.9367	29378.65259
V37	12.76901625	167277703.4	165157.82	12934.26343
V38	12.80189853	291201864.4	280736.8585	21929.31445
V39	12.83486549	295481530	278252.9901	21679.46289

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

V40	12.86791734	386230024.4	355396.923	27618.83789
V41	12.9010543	160382847.1	144255.3183	11181.66895
V42	12.9342766	229659909.2	201979.8698	15615.86133
V43	12.96758445	135598954.8	116644.9035	8995.114235
V44	13.00097807	173402815.8	145943.4983	11225.57838
V45	13.03445769	389799340	321082.6985	24633.3761
V46	13.06802352	404957156.7	326554.5182	24988.82234
V47	13.10167579	161947710.6	127882.665	9760.786865
V48	13.13541472	71261624.51	55118.61376	4196.183746
V49	13.16924054	447369669.5	339020.9041	25743.39069
V50	13.20315346	473399199.5	351570.8815	26627.79636
V51	13.23715371	5021332.437	3655.395883	276.1466675

Table 2 : After decryption the Candidates Private Key Rj and Voters Private Key Yi

Common Key CK_i	**Decryption of voters choices $D(EC_i)=PC_j*PV_i$**	**Pseudony-mous of voters PV_i**	**Pseudony- mous of candidates PC_j**	**Candidates Private Key R_j**	**Voters Private key Y_i**
252.5437073	104701.8251	11.63985497	8995.114235	27.04252503	11.63985497
270.8111652	131000.5854	11.66982947	11225.57838	27.41434397	11.66982947
289.2269642	288207.5731	11.69988117	24633.3761	27.7912752	11.69988117
307.7923091	293119.1421	11.73001025	24988.82234	28.17338901	11.73001025
326.5084141	114788.9708	11.76021692	9760.786865	28.56075667	11.76021692
345.3765037	49475.11023	11.79050137	4196.183746	28.9534504	11.79050137
364.3978118	304309.1155	11.82086382	25743.39069	29.35154345	11.82086382
383.5735828	315574.1215	11.85130445	26627.79636	29.75511004	11.85130445
402.905071	3281.125956	11.88182347	276.1466675	30.16422544	11.88182347
422.3935409	51363.01444	11.91242109	4311.719177	30.57896593	11.91242109
442.0402672	117148.3081	11.94309749	9808.87146	30.99940887	11.94309749
461.846535	315379.6352	11.9738529	26339.02704	31.42563265	11.9738529
481.8136401	72665.79929	12.0046875	6053.118774	31.85771676	12.0046875
501.9428883	349520.5144	12.03560151	29040.55225	32.29574177	12.03560151
522.2355964	354500.3061	12.06659513	29378.65259	32.73978937	12.06659513
542.6930918	156474.432	12.09766856	12934.26343	33.18994237	12.09766856
563.3167127	265976.7517	12.12882201	21929.31445	33.64628471	12.12882201
584.107808	263623.4759	12.16005568	21679.46289	34.10890148	12.16005568
605.0677378	336711.4658	12.19136979	27618.83789	34.57787897	12.19136979
626.197873	136670.9066	12.22276453	11181.66895	35.05330463	12.22276453
647.4995958	191360.5144	12.25424012	15615.86133	35.53526711	12.25424012
668.9742997	110512.1454	12.28579677	8995.114235	27.04252503	12.28579677
690.6233892	138270.3284	12.31743468	11225.57838	27.41434397	12.31743468
712.4482806	304201.3565	12.34915406	24633.3761	27.7912752	12.34915406
734.4504013	309385.4881	12.38095513	24988.82234	28.17338901	12.38095513
756.6311907	121159.0669	12.41283808	9760.786865	28.56075667	12.41283808
778.9920995	52220.68069	12.44480315	4196.183746	28.9534504	12.44480315
801.5345904	321196.4375	12.47685052	25743.39069	29.35154345	12.47685052
824.2601381	333086.5834	12.50898043	26627.79636	29.75511004	12.50898043
847.1702289	3463.208673	12.54119307	276.1466675	30.16422544	12.54119307
870.2663615	54213.35221	12.57348867	4311.719177	30.57896593	12.57348867

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

893.5500467	123649.3333	12.60586743	9808.87146	30.99940887	12.60586743
917.0228074	332881.3044	12.63832957	26339.02704	31.42563265	12.63832957
940.686179	76698.31324	12.67087531	6053.118774	31.85771676	12.67087531
964.5417095	368916.7966	12.70350486	29040.55225	32.29574177	12.70350486
988.5909592	374172.9367	12.73621844	29378.65259	32.73978937	12.73621844
1012.835501	165157.82	12.76901625	12934.26343	33.18994237	12.76901625
1037.276922	280736.8585	12.80189853	21929.31445	33.64628471	12.80189853
1061.916819	278252.9901	12.83486549	21679.46289	34.10890148	12.83486549
1086.756805	355396.923	12.86791734	27618.83789	34.57787897	12.86791734
1111.798504	144255.3183	12.9010543	11181.66895	35.05330463	12.9010543
1137.043555	201979.8698	12.9342766	15615.86133	35.53526711	12.9342766
1162.493609	116644.9035	12.96758445	8995.114235	27.04252503	12.96758445
1188.150331	145943.4983	13.00097807	11225.57838	27.41434397	13.00097807
1214.015398	321082.6985	13.03445769	24633.3761	27.7912752	13.03445769
1240.090503	326554.5182	13.06802352	24988.82234	28.17338901	13.06802352
1266.377351	127882.665	13.10167579	9760.786865	28.56075667	13.10167579
1292.877662	55118.61376	13.13541472	4196.183746	28.9534504	13.13541472
1319.59317	339020.9041	13.16924054	25743.39069	29.35154345	13.16924054
1346.525621	351570.8815	13.20315346	26627.79636	29.75511004	13.20315346
1373.676778	3655.395883	13.23715371	276.1466675	30.16422544	13.23715371

Here the public key Yi of the voter Vi and candidates Cj from that it can easily verified the voter's choice wherever necessary for the sample random case. This can achieve the confidence of the every voters that casted vote counted correctly in the final tally but this data are kept confidential and tested on for the some random cases for the privacy point of view of the voters. The each voter has his separate common key for the encryptions and descriptions.

VII. UNIVERSAL VERIFICATION BY THE POLITICAL AND OTHER ORGANIZATIONS

Every after casting a vote Vi he / she gets ((Id, Xi, Yi, PVi, SGi, Bm, CKi, VKCi, ECi) this nine code generated by system. Out of this voter Id, secrete key Xi, private key Yi are created by competent election authority before the election. The pseudonymous PVi of every voter generated for the election purpose to hide the voter's real identity. SGi is the system signature created by the agreement of three groups A, B and C and voter Vi that can be used for the authentication of the voter and which are the encryption by three secrete key Xa, Xb and Xc of voters private key Yi.

Thus any political party can verify the legality of voter pseudonymous PVi with this SGi, also the signatures are different for the different voter Vi. This can be verify by the declaration in the bulletin board BB of the pair (VKCi and SGi) and the VKCi is the encryption of the PVi hence that cannot identify the any link to the voter.

The main purpose of the verification of any political party and the any non-political organizations are the votes of their party are counted correctly by the system or not. This can be achieved by the ECi after decrypting it. The decryption can be possible by the common key CKi.

Where

$$CKi = Q\ Xi\ Xa\ Xb\ Xc \bmod P;$$

Decryption by CKi as

$$DCKi\ (ECi) = DCK\ (ECK\ (PCj * PVi));$$
$$[ECi = ECKi\ (PCj * PVi)]$$
$$= PCj * PVi;$$

The product of the pseudonymous PCj and PVi which is PCj * PVi are the best proof to verify the link between voter and the candidates after counting.

$$PCj = (PCj * PVi) / PVi$$

Table 3 gives the details about the verification:

Votes V_i	Common key CK_i	Decryption D(ECi)=PCi*PVi	Pseudonymous Of candidates PC_J	Public key of candidates R_J	Public key of voter Y_i
V1	252.5437073	104701.8251	8995.11423	27.04252503	11.63985497
V2	270.8111652	131000.5854	11225.5784	27.41434397	11.66982947
V3	289.2269642	288207.5731	24633.3761	27.7912752	11.69988117
V4	307.7923091	293119.1421	24988.8223	28.17338901	11.73001025
V5	326.5084141	114788.9708	9760.78687	28.56075667	11.76021692

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

V6	345.3765037	49475.11023	4196.18375	28.9534504	11.79050137
V7	364.3978118	304309.1155	25743.3907	29.35154345	11.82086382
V8	383.5735828	315574.1215	26627.7964	29.75511004	11.85130445
V9	402.905071	3281.125956	276.146667	30.16422544	11.88182347
V10	422.3935409	51363.01444	4311.71918	30.57896593	11.91242109
V11	442.0402672	117148.3081	9808.87146	30.99940887	11.94309749
V12	461.846535	315379.6352	26339.027	31.42563265	11.9738529
V13	481.8136401	72665.79929	6053.11877	31.85771676	12.0046875
V14	501.9428883	349520.5144	29040.5522	32.29574177	12.03560151
V15	522.2355964	354500.3061	29378.6526	32.73978937	12.06659513
V16	542.6930918	156474.432	12934.2634	33.18994237	12.09766856
V17	563.3167127	265976.7517	21929.3145	33.64628471	12.12882201
V18	584.107808	263623.4759	21679.4629	34.10890148	12.16005568
V19	605.0677378	336711.4658	27618.8379	34.57787897	12.19136979
V20	626.197873	136670.9066	11181.6689	35.05330463	12.22276453
V21	647.4995958	191360.5144	15615.8613	35.53526711	12.25424012
V22	668.9742997	110512.1454	8995.11423	27.04252503	12.28579677
V23	690.6233892	138270.3284	11225.5784	27.41434397	12.31743468
V24	712.4482806	304201.3565	24633.3761	27.7912752	12.34915406
V25	734.4504013	309385.4881	24988.8223	28.17338901	12.38095513
V26	756.6311907	121159.0669	9760.78687	28.56075667	12.41283808
V27	778.9920995	52220.68069	4196.18375	28.9534504	12.44480315
V28	801.5345904	321196.4375	25743.3907	29.35154345	12.47685052
V29	824.2601381	333086.5834	26627.7964	29.75511004	12.50898043
V30	847.1702289	3463.208673	276.146667	30.16422544	12.54119307
V31	870.2663615	54213.35221	4311.71918	30.57896593	12.57348867
V32	893.5500467	123649.3333	9808.87146	30.99940887	12.60586743
V33	917.0228074	332881.3044	26339.027	31.42563265	12.63832957
V34	940.686179	76698.31324	6053.11877	31.85771676	12.67087531
V35	964.5417095	368916.7966	29040.5522	32.29574177	12.70350486
V36	988.5909592	374172.9367	29378.6526	32.73978937	12.73621844
V37	1012.835501	165157.82	12934.2634	33.18994237	12.76901625
V38	1037.276922	280736.8585	21929.3145	33.64628471	12.80189853
V39	1061.916819	278252.9901	21679.4629	34.10890148	12.83486549
V40	1086.756805	355396.923	27618.8379	34.57787897	12.86791734
V41	1111.798504	144255.3183	11181.6689	35.05330463	12.9010543
V42	1137.043555	201979.8698	15615.8613	35.53526711	12.9342766
V43	1162.493609	116644.9035	8995.11423	27.04252503	12.96758445
V44	1188.150331	145943.4983	11225.5784	27.41434397	13.00097807
V45	1214.015398	321082.6985	24633.3761	27.7912752	13.03445769
V46	1240.090503	326554.5182	24988.8223	28.17338901	13.06802352
V47	1266.377351	127882.665	9760.78687	28.56075667	13.10167579
V48	1292.877662	55118.61376	4196.18375	28.9534504	13.13541472
V49	1319.59317	339020.9041	25743.3907	29.35154345	13.16924054
V50	1346.525621	351570.8815	26627.7964	29.75511004	13.20315346
V51	1373.676778	3655.395883	276.146667	30.16422544	13.23715371

Table 3: Pseudonymous of candidates PC_J and corresponding Public key of Candidates R_J and Public key of voter Y_i

VIII. CONCLUSION

Verifications of the voting process conducted by election authority by the e-process through internet as on line election process are essential part of the systems. From the above table prove that while preserving the voters privacy it is also possible to verify individually and universally. That the voters casting their votes are counted in the final tally as per the intension of the voters. And also satisfy by the verification of the election process any political party or any interested social group that the recorded votes are counted correctly the final tally at any phase of the on line election process.

IX. REFERENCES

[1]. 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

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

, Transactions on Volume: 4 , Issue: 4 , Part: 1, Page(s): 597 – 610.

[2]. Yasinsac, A.; Bishop, M.; "Of Paper Trails and Voter Receipts" Hawaii International Conference on System Sciences, Proceedings of the 41st Annual 7-10 Jan. 2008 Page(s):487 – 487.

[3]. Langer, L.; Schmidt, A.; Buchmann, J.; Volkamer, M.; Stolfik, A.; "Towards a Framework on the Security Requirements for Electronic Voting Protocols", First IEEE International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE), 2009, Page(s): 61 – 68.

[4]. Alberdi, E.; Strigini, L.; Leach, K.; Ryan, P.; Palanque, P.; Winckler, M.;" Gaining Assurance in a Voter-Verifiable Voting System" , Second International IEEE Conference on Dependability, 2009. DEPEND '09; 2009, Page(s): 99 – 104.

[5]. 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.

[6]. 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.

[7]. Villafiorita, A.; Weldemariam, K.; Tiella, R.; "Development, Formal Verification, and Evaluation of an E-Voting System With VVPAT"; Information Forensics and Security, IEEE Transactions on Volume: 4, Issue: 4 , Part: 1, 2009 Page(s): 651 – 661.

[8]. Campanelli, S.; Falleni, A.; Martinelli, F.; Petrocchi, M.; Vaccarelli, A.;" Mobile Implementation and Formal Verification of an e-Voting System", Internet and Web Applications and Services, 2008. ICIW '08. Third International IEEE Conference on Digital Object Identifier, 2008, Page(s): 476 – 481.

[9]. D. Chaum , Secret-Ballot Receipts: True Voter verifiable Electronic , IEEE Security and Privacy , 2(1): 38-47, 2004.

[10]. 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.

[11]. Kaminski, H.; Kari, L.; Perry, M.;"Who counts your votes?" [VEV electronic voting system] e-Technology, e-Commerce and e-Service, 2005. EEE '05. Proceedings. The 2005 IEEE International Conference on 29 March-1 April 2005 Page(s):598 – 603.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html