ISSN:2231-0711

P.Lakshmi et al | IJCSET(www.ijcset.net) | June 2016 | Vol 6, Issue 6, 179-184

Customized Elliptic Curve Cryptography Based Ant Colony Optimization for Internet Polling System

Mrs.P.Lakshmi, M.Sc.,M.Phil.,UGC-NET.,[#1], J. Vidhyanandhini[*2]

[#] *Assistant professor, Deportment of Computer Science and MCA,*
Information Technology and Application
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

[*]*Research Scholar*
Research Scholar, Department of Computer Science
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

Abstract— **The hopeful determination framework is requiring of each majority rule government and the organization shaped is reliant on the consequences of the applicant choice. The competitor determination process clears the way for each voter to choose a delegate among themselves who can manage the just framework towards the welfare of the general public. The Polling framework has watched numerous viable changes in the course of recent decades, right from the conventional paper ticket surveying to electronic Polling and now towards the Internet Polling. Be that as it may, the balloter decision is a dependable and certain Polling where in manual framework he used to stamp on his preferred image. This requires a security calculation that could oppose the assaults and keep the information secrecy furthermore validate Elector in on the web. Modified Elliptic Curve Cryptography is utilized for both authentication and confidentiality. Parallel Multi-core Ant colony optimization is utilized to produce the private keys utilized as a part of ECC by ideally utilizing multi-core processors.**

Keywords— **Internet Polling (I-Polling), electronic Polling, data confidentiality, authenticate elector, Modified Elliptic Curve Cryptography (MECC), Parallel Multi-core Ant colony optimization (PMACO.**

I. INTRODUCTION

Surveying is the system utilized by any qualified balloter to choice his decision from a rundown of competitors. Competitor choices are directed all around from little union hopeful choice keeping in mind the end goal to choose a pioneer to immense general applicant determinations to choose the leader or president. This is utilized all around, for example, school delegates, school agents, union pioneer, national or state pioneer. Surveying is required to be directed in different circumstances. Any place competitor choice frameworks are led, the hopeful choice framework must be hearty and secure which ought to oppose an assortment of fake activities [1] [2]. This is required to be straightforward and understandable that voters and hopefuls ought to acknowledge the consequences of the applicant determination with no issue. In any case, when we allude to past connections, some cases have huge impact on directing the hopeful choice easily and had impact on the outcome that is inadmissible. A secured Polling framework needs to meet the accompanying criteria [3].

- There are some assaults from controlled persons which incorporate poll stuffing and wrong checking by couple of persons inside tallying focus.
- Secrecy of vote is critical and it ought to ensure the balloter security which has no confirmation appearing to which applicant Poll is threw by the voter.
- The framework ought to be adaptable and justifiable by a wide range of electorate. Each voter ought to have the capacity to cast his Poll either matured or debilitated.
- The general Polling procedure ought to be reasonable and compelling and voter ought to feel that the whole framework is honest to goodness.
- Authentication of voter is must as the correct individual ought to make the choice. 6. Pace and Accuracy are additionally imperative in accomplishing secure Polling.

As the part of Internet Polling framework is pivotal, it is hard to think of a framework which is very secure and exact in all detects. In the event that these variables of security are fulfilled, then Internet Polling could be an incredible change over paper frameworks and EVMs [4].

II. MODIFIED ELLIPTIC CURVE CRYPTOGRAPHY PARALLEL MULTI CORE ANT COLONY OPTIMIZATION (PMACO)

The ant colony advancement taking into account the transformative system of calculation that improves a target capacity by performing populace based hunt. The ants in populace that are potential arrangements are like winged animals in a herd. The ants are initially instated arbitrarily and after that fly over the multi-dimensional hunt space. Each ant redesigns its speed and position in light of its own best experience and that of the whole populace. The overhauling approach will bring about the ant swarm to move toward a district with higher item esteem [5]. Parallel Multi-core preparing plans to deliver the same results by utilizing numerous processors that at last expands the CPU usage [6]. In this study, the soul of the information parallelism strategy was used to make a parallel ant swarm improvement (PACO) calculation. The motivation behind

applying parallel preparing to ant swarm advancement goes more distant than only being an equipment quickening agent. Or maybe, a disseminated plan is produced which gives better arrangements with diminished general calculation. It is hard to discover a calculation which is proficient and viable for a wide range of issues. Our exploration has demonstrated that the execution of PACO can be profoundly reliant on the level of connection amongst's parameters and the way of the correspondence system. In PMACO the ants redesign its speed and position by utilizing the accompanying condition which signifies kth emphasis with n cores. The numerical type of the parallel ant swarm improvement calculation can be communicated as appeared in condition (1) and (2) [7].

$$V_{1,m}^{k+1} = wV_{1,n}^{k} + F_1 \times r_1 \times \left(P_{best,n} - U_{1,n}^{k}\right) + F_2 \times r_2 \times \left(G_{best} - U_1^{k}\right)$$

$$U_{1,n}^{k+1} = U_{1,n}^{k} + V_{1,n}^{k+1}$$

Here V1, nk speaks to the Velocity of specialist at kth emphasis at nth core and V1, nk+1 at next cycle. U1, nk is the present position of the specialist at kth emphasis at nth core and U1, nk+1 at next cycle. Gbest is the best position among all ants from the first to keep going cycle basing on the quantity of cores which are needy upon framework being executed. The complete calculation for PMACO is given underneath and the figure 1 delineates the flowchart.

Step 1 : Initialize every ant

Step 2 : Repeat step 1 until all ants are introduced

Step 3: Calculate Fitness esteem for every ant applying multi-core parallel handling.

Step 4 : Check if wellness worth is superior to anything ants individual best esteem in every core

Step 5 : Set ants best esteem as present pbest.

Step 6 : Calculate parallel individual best pbest. [End of Step4 if statement]

Step 7 : Repeat Step 3 through 6 until all ants are computed.

Step 8 : Select gbest (worldwide best) with the best wellness esteem among all ant.

Step 9 : Update speed of every ant by utilizing condition 7.

Step 10 : Update position of every ant by utilizing condition 8.

Step 11 : Repeat Step 6 and 7 until all ants are upgraded.

Step 12 : Repeat Step 2 through 8 until least mistake or most extreme cycles.

A. Advantage of PMACO

1. Simple to Implement and basic
2. Accomplishes arrangement quicker.
3. Connected to Engineering furthermore Scientific Problems as this depends on insight.
4. Contrasted with GA this has no covering and transformation figuring. Pursuit depends on computing the speed of ant.
5. Utilizes genuine number code and the quantity of measurements are equivalent to steady of arrangement.
6. Viably uses processor abilities.

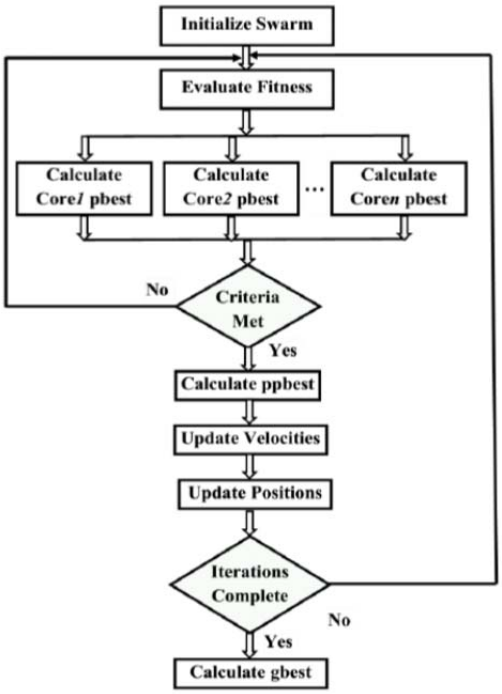


FIGURE 1: MULTI-CORE PARALLEL ACO FLOWCHART.

III. MODIFIED ELLIPTIC CURVE CRYPTOGRAPHY

Here ECC and PMACO are joined where the parameters in ECC are picked by utilizing PMACO. This uses the ideas of open key cryptography that includes both private and open keys and elliptic bend. The private keys are picked by improvement calculation PMACO.

A. MECC Discrete Logarithm Problem

The Whenever P and Q are known, discover k such that Q=kP. This issue is known as the discrete logarithm issue for elliptic bends which is accepted to be a "difficult" issue, in that there is no known polynomial time calculation that can keep running on an established PC [8]. DLP is likewise accessible in different cryptosystems, for example, the Digital Signature Algorithm (DSA), ElGamal calculation and the Diffie-Hellman key trade (DH) [9]. However in ECC the discrete logarithm issue for elliptic bends is by all accounts harder if contrasted with other comparable issues utilized as a part of cryptography. This suggests we require less bits for the whole number k keeping in mind the end goal to accomplish the same level of security as with different cryptosystems [9][10].

B. Authentication with MECC

The verification utilizing MECC is as appeared as a part of beneath strategy

1. Two clients An and B select the elliptic bend parameters.
2. Administrator B takes an arbitrary point Message Point, MP on the chose elliptic bend which is transmitted to Voter.
3. Voter A chooses his private key PrA utilizing PMACO calculation which is kept safely with him.

4. Voter figures his open key point by utilizing his private key and applying scalar augmentation on elliptic bend point MP basing on condition 3 and sends to Admin

PuA = PrA x MP … (3)

5. Also, Admin chooses his private key utilizing PMACO calculation PrB that is kept safely with client B.

6. Client B figures his open key point utilizing his private key and taking into account condition 4 and sends to User A

Bar = PrB x MP … (4)

7. Administrator registers last point basing on condition 5

Dad = PrA x PuB … (5)

8. Balloter processes last point basing on condition 6

Pb = PrB x PuA … (6)

9. This actualizes the idea of shared mystery key as appeared in condition 7

Dad = kaR = kakbP = kbkaP = kbQ = Pb … (7).

C. Encryption with MECC

1. Balloter chooses his private key his private key utilizing PMACO calculation which is any arbitrary number Pra. 2. At that point he figures his open key from private key and sends that to Admin basing on condition 8 and which is another point on elliptic bend.

Q = nPb … (8)

3. Voter signs with private key

4. Administrator checks on the off chance that he is substantial balloter and he sends his open key PuA to voter.

5. Voter encodes his Poll utilizing the administrator's open key PuA.

6. Administrator decodes the voter's decision utilizing his private key PrA

D. MECC Advantages

Contrasted with customary frameworks, MECC calculations have taking after favorable circumstances [12] [13]

1. Short Keys
2. Snappy Processing
3. Same bend can be utilized for a few unmistakable key sets.
4. Used to element whole numbers
5. Guarantees Integrity, Authentication and Confidentiality

IV. RELIABLE AND VERIFIED INTERNET POLLING SYSTEM USING MECC

The Reliable Internet Polling is conceivable by applying the accompanying technique.

1. Confirm Elector by utilizing ECC
2. Scramble Poll by utilizing MECC
3. Confirm Poll by applying the methodology given underneath.

Balloter may get a kick out of the chance to confirm the Poll whether it is transmitted accurately and his decision is effectively tallied. This requires a system where the balloter is verified and encoded Poll is send to voter which is unscrambled by utilizing his private key [14][15].

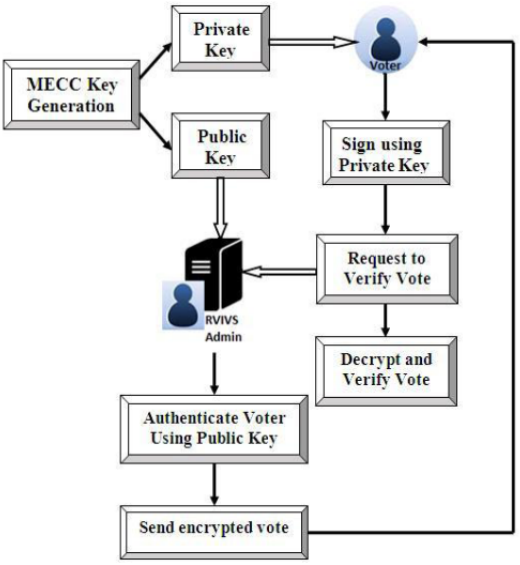


FIGURE 2: PROPOSED FLOWCHART FOR INTERNET POOLING SYSTEM

Balloter picks his private key which is any arbitrary number nv. At that point he figures his open key from private key and sends that to Admin elliptic bend. Balloter signs with private key and Admin checks in the event that he is substantial voter and he sends open key to voter. Voter solicitations to confirm his vote. Administrator encodes Poll utilizing the voter's open key. Voter unscrambles Poll utilizing his private key to check that his Poll is numbered to his preferred applicant [16] [17].

V. RESULTS AND DISCUSSIONS

To keep up the security of the framework, the voter needs to assume the liability in keeping his private key secure. The channel additionally ought to be secure while transmitting the keys, such a variety of times hashing and encryption calculations is connected to the private key to guarantee non-revocation and respectability. The proposed calculation is produced and is tried on a case situation. For this situation the picked elliptic bend is plotted in Fig 3. At that point verification is connected and the table 1 demonstrates the ECC results. Here MP is the Message Point and PrA the private key of An and PrB the private key of B. PuA and PuB are open keys of An and B figured from private keys utilizing ECC operations. Dad and PB are processed at both the closures utilizing ECC operations to check for validation which constantly same. Notwithstanding, it can be watched that PA and PB are now and again achieving unending qualities in ECC operations as they are going past the reach.

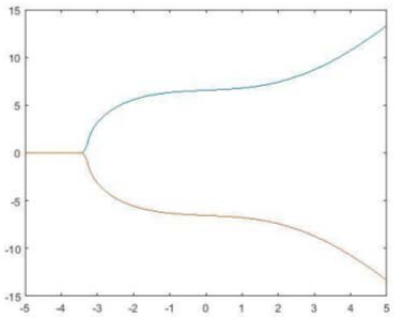
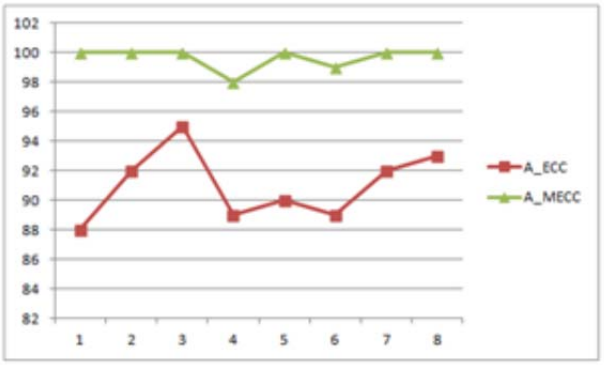
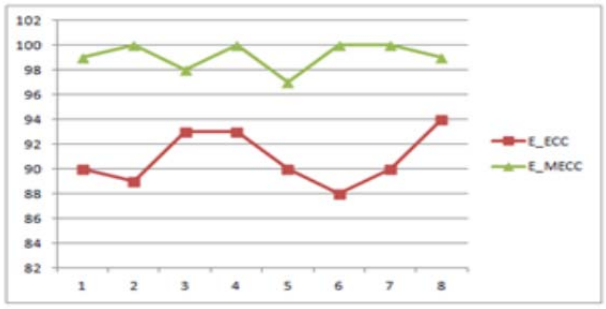


Figure 3: $x^3+2x+43$

This is comparative if there should arise an occurrence of calculation connected in validation and encryption achievement rate is constantly high in MECC contrasted with ECC. The figure 4 demonstrates the test results on both calculations. The perceptions portray that both calculations identified with confirmation and encryption utilizing MECC are dependably exceedingly exact contrasted with those utilizing ECC.



(a) Authentication using ECC and MECC



(b) Encryption using ECC and MECC

Figure 4: Authentication and Encryption and Success Rate on test sets

At that point verification is connected and the table 1 demonstrates the ECC results. Here MP is the Message Point and PrA the private key of An and PrB the private key of B. PuA and PuB are open keys of An and B processed from private keys utilizing ECC operations. Dad and PB are processed at both the finishes utilizing ECC operations to check for verification which constantly same. Nonetheless, it can be watched that PA and PB are some of the time achieving boundless qualities in ECC operations as they are going past the reach.

TABLE 1: AUTHENTICATION PARAMETERS OF ECC ON X3+2X+43 MOD 17

MP	PrA	PrB	PuA	PuB	PA	PB
[126896, 10]	100547	33889	[15, 6]	[4, 1]	[12, 10]	[12, 10]
[78205, 8]	45121	86131	[5, 9]	[5, 8]	[5, 9]	[5, 9]
[13374, 10]	14551	69401	[6, 15]	[6, 2]	[8, 10]	[8, 10]
[67966, 9]	47881	125201	[67966, 9]	[67966, 9]	[67966, 9]	[67966, 9]
76929, 13]	78163	51461	[8, 9]	[4, 4]	[8, 8]	[8, 8]
[24014, 9]	117979	25457	[7, 9]	[24014, 9]	[7, 9]	[7, 9]
[39398, 8]	128393	89563	[9, 8]	[9, 8]	[9, 8]	[9, 8]
[97862, 9]	87359	85847	[10, 8]	[1, 4]	[1, 13]	[1, 13]
[68669, 16]	1733	27077	[15, 4]	[15, 4]	[16, 5]	[16, 5]
[11980, 10]	6779	97021	[4, 16]	[12, 10]	[4, 16]	[4, 16]
[123565, 8]	953	3673	[5, 8]	[9, 9]	[5, 9]	[5, 9]
[31361, 5]	81637	92623	[16, 3]	[6, 6]	[13, 5]	[13, 5]
[43128, 6]	123979	163	[16, 6]	[16, 6]	[16, 6]	[16, 6]
[9838, 10]	75553	116483	[15, 6]	[8, 7]	[6, 15]	[6, 15]
[27157, 10]	49999	90437	[15, 11]	[6,15]	[4, 16]	[4, 16]
[12183, 2]	11549	80909	[11, 15]	[15, 4]	[15, 13]	[15, 13]
[53013, 9]	59581	80809	[10, 8]	[15, 1]	[1, 4]	[1, 4]
[74615, 4]	109397	117619	[7, 15]	[16, 1]	[2, 13]	[2, 13]
[20567, 10]	10177	32299	[5, 9]	[2, 14]	[9, 8]	[9, 8]
[31545, 9]	93323	48527	[7, 9]	[10, 8]	[7, 8]	[7, 8]
[71559, 16]	104831	113417	[6, 16]	[11, 2]	[11, 2]	[11, 2]
[62709, 5]	112459	117361	[6, 6]	[13, 5]	[6, 6]	[6, 6]
[98065, 8]	2143	47441	[14, 7]	[14, 7]	[5, 9]	[5, 9]
[58245, 8]	70891	86453	[9, 9]	[9, 8]	[5, 8]	[5, 8]

TABLE 2: AUTHENTICATION PARAMETERS OF MECC ON X3+2X+43 MOD 17

MP	PrA	PrB	PuA	PuB	PA	PB
[126896, 10]	100547	33889	[15, 6]	[4, 1]	[12, 10]	[12, 10]
[78205, 8]	45121	86131	[5, 9]	[5, 8]	[5, 9]	[5, 9]
[13374, 10]	14551	69401	[6, 15]	[6, 2]	[8, 10]	[8, 10]
[67966, 9]	47881	125201	[67966, 9]	[67966, 9]	[67966, 9]	[67966, 9]
76929, 13]	78163	51461	[8, 9]	[4, 4]	[8, 8]	[8, 8]
[24014, 9]	117979	25457	[7, 9]	[24014, 9]	[7, 9]	[7, 9]
[39398, 8]	128393	89563	[9, 8]	[9, 8]	[9, 8]	[9, 8]
[97862, 9]	87359	85847	[10, 8]	[1, 4]	[1, 13]	[1, 13]
[68669, 16]	1733	27077	[15, 4]	[15, 4]	[16, 5]	[16, 5]
[11980, 10]	6779	97021	[4, 16]	[12, 10]	[4, 16]	[4, 16]
[123565, 8]	953	3673	[5, 8]	[9, 9]	[5, 9]	[5, 9]
[31361, 5]	81637	92623	[16, 3]	[6, 6]	[13, 5]	[13, 5]
[43128, 6]	123979	163	[16, 6]	[16, 6]	[16, 6]	[16, 6]
[9838, 10]	75553	116483	[15, 6]	[8, 7]	[6, 15]	[6, 15]
[27157, 10]	49999	90437	[15, 11]	[6,15]	[4, 16]	[4, 16]
[12183, 2]	11549	80909	[11, 15]	[15, 4]	[15, 13]	[15, 13]
[53013, 9]	59581	80809	[10, 8]	[15, 1]	[1, 4]	[1, 4]
[74615, 4]	109397	117619	[7, 15]	[16, 1]	[2, 13]	[2, 13]
[20567, 10]	10177	32299	[5, 9]	[2, 14]	[9, 8]	[9, 8]
[31545, 9]	93323	48527	[7, 9]	[10, 8]	[7, 8]	[7, 8]
[71559, 16]	104831	113417	[6, 16]	[11, 2]	[11, 2]	[11, 2]
[62709, 5]	112459	117361	[6, 6]	[13, 5]	[6, 6]	[6, 6]
[98065, 8]	2143	47441	[14, 7]	[14, 7]	[5, 9]	[5, 9]
[58245, 8]	70891	86453	[9, 9]	[9, 8]	[5, 8]	[5, 8]

Table 2 demonstrates the MECC resultant information. Parameters are comparable as indicated in table 1. Be that as it may, the qualities in elliptic bend are upgraded utilizing PMACO. Subsequently it is plainly watched that PA and PB are dependably inside the extent

VI. CONCLUSIONS

Surveying is the procedure required at whatever point there is more than one individual seeking any position or proclamations or perspectives to be picked among different decisions. The Polling framework is enhancing regulated; headway in the new framework disposes of the downsides of the past framework. Each framework tries to defeat the escape clauses of the past framework. The proposed security calculation is very precise in both the cases verification and privacy. However security is not constrained to an application and consequently this can be reached out to applications wherever there is necessity of uprightness, classification and validation. Other advancement procedures can likewise be utilized to ideally pick the private keys in ECC.

REFERENCES

[1] Daniel Barbara and Hector Garcia-Molina, “The Reliability of Voting Mechanisms”, IEEE, vol. c-36, pp. 1197-1208, (1987).

[2] Behrooz Parhami, “Voting Algorithms”, IEEE, vol 43, No 4, pp. 617-629, (1994).

[3] Orhan Centinkoya, “Analysis of Security Requirement of Cryptographic Voting Protocols(Extended Abstract)”, IEEE, pp. 1451-1456, (2008).

[4] K. Sujatha, P. V. Nageswara Rao, A. Arjuna Rao, L. V. Rajesh, V. Vivek Raja; “Secured Internet Voting System based on Combined DSA and Multiple DES Algorithms”, ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II Advances in Intelligent Systems and Computing Volume 249, 2014, pp 643-650.

[5] Liangjun Ke, Zuren Feng, Zhigang Ren, "An Efficient ant colony optimization approach to attribute reduction in rough set theory", Pattern Recognition Letter, Volume 29, Issue 9, July 2008, pp.1351-1357.

[6] Sujatha, K. ; Nageswara Rao, P. V. ; Rao, A. A. ; Sastry, V. G. more authors “Multicore Parallel Processing Concepts for Effective Sorting and Searching”, Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on 2-3 Jan. 2015, IEEE, pp 162 – 166.

[7] Yijum He, Dezhao Chen and Weixiang Zhao, "Ensemble Classifier system based on ant colony algorithm and its application in chemical pattern classification", Chemometrics and Intelligent Laboratory, Volume 80, Issue 1, January 2006, pp.39-49.

[8] Neal Koblitz, “Elliptic Curve Cryptosystems”, MATHEMATICS OF COMPUTATION, Vol 48. Number 177, Jan I987. pp 203-209.

[9] William Stallings, “Cryptography and Network Security-Principles and Practices”, Fourth Edition, P, earson 2007.
[10] Victor S. Miller, “Use of Elliptic Curves in Cryptography”, LNCS, Advances in Cryptology — CRYPTO ’85 Proceeding, Sec V, pp 417-426, 1986, Springer Berlin Heidelberg.
[11] Amara M, Siad A. , “Elliptic Curve Cryptography and its applications”, Systems, Signal Processing and their Applications (WOSSPA), 2011 7th International Workshop, May 2011, pp 247 – 250, IEEE.
[12] Qizhi Qiu, QianXing Xiong, “Research on elliptic curve cryptography”, Computer Supported Cooperative Work in Design, 2004. Proceedings. The 8th International Conference on (Volume:2), May 2004, pp 698 - 701 Vol. 2, IEEE.
[13] Qiuxia Zhang, Zhan Li ; Chao Song, “The Improvement of digital signature algorithm based on elliptic curve cryptography”, Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference, Aug. 2011, pp 1689 – 1691, IEEE.
[14] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, “Analysis of an Electronic Voting System”, IEEE Symposium, pp. 27-40, (2004).
[15] Frank B Ryan, “The Electronic Voting System for the United States House of Representatives”, IEEE, vol. 5, pp. 32-37, (1972).
[16] Costas Lambrinoudakis, et. al, “Electronic Voting Systems: Security Implications of the Administrative Workflow” , IEEE, pp. 467-471, (2003).
[17] Indrajit Ray, Indrakshi Ray and Natarajan Narasimhamurthi, “An Anonymous Electronic Voting Protocol for Voting Over The Internet”, IEEE, pp. 1-6, (2001).