ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

Detailed Implementation of E-Voting System for on Duty Persons using RSA Algorithm with Kerberos Concept

Ms. Tanzila Afrin[1], Prof.K.J.Satao[2]

M.Tech Scholar, Dept. of Computer Science & Engineering,Rungta College of Engineering & Technology, Bhilai (C.G.),India.

HOD,Dept. of Information Technology,Rungta College of Engineering & Technology, Bhilai (C.G.),India.

ABSTRACT**:** An electronic voting (e-voting) system is a voting system in which the election data is stored, recorded and processed primarily as digital information. There are lots of security challenges associated with the use of Internet voting solutions. Authentication of Voters, safety of voting process, Securing voted records are the main challenge of e-voting. This E-Voting system mainly for those people who are public servants they are not capable to come to the voting booth due to on duty. In voting system there are some important processes. This system having main four processes: first one is application control process which involves the identification and authentication phases for the applied citizens. Second one is the voting process which will be done by voter. In Third section confirmation process, in this system check scan copy of voter ID and passport size photograph send by voter. Finally the election server, administrator will sort out valid voter, schedule date of election and display final result by decipher the received encrypted information using public key cryptography.

Keyword:-Encryption, Decryption, RSA, public key, E-voting, KDC, TGS.

Abstract: An electronic voting (e-voting) system is a voting system in which the election data is stored, recorded and processed primarily as digital information. There are lots of security challenges associated with the use of Internet voting solutions. Authentication of Voters, safety of voting process, Securing voted records are the main challenge of e-voting. This E-Voting system mainly for those people who are public servants they are not capable to come to the voting booth due to on duty. In voting system there are some important processes. This system having main four processes: first one is application control process which involves the identification and authentication phases for the applied citizens. Second one is the voting process which will be done by voter. In Third section confirmation process, in this system check scan copy of voter ID and passport size photograph send by voter. Finally the election server, administrator will sort out valid voter, schedule date of election and display final result by decipher the received encrypted information using public key cryptography.

Keyword:-Encryption, Decryption, RSA, public key, E-voting, KDC, TGS.

I. INTRODUCTION

A. *Voting System:*

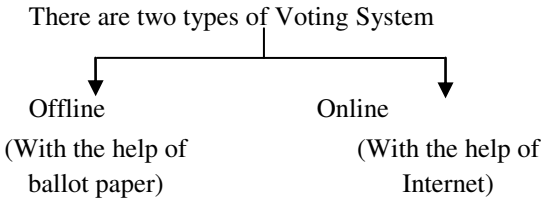
Voting process plays an important role in any democracy contrary. Democracy is to allow people to vote freely and the election result is accepted by voters group. There is an important motivating factor in the introduction of electronic voting is the elimination of election forms.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013



Drawback of Offline voting system:

- In offline voting system physical presence is required along with identification.
- Offline voting system is generally divided into paper work.
- Time consuming.
- Takes long time for declaring result.

Advantage of Online voting system:

- Voters are able to vote from any ware without going to voting booth. Mainly save votes of those people who are not capable to come to the voting booth due to on duty reason, or the people who are physically handicapped.
- Less paper work
- Save time.
- Providing fast voting result.

This paper is about online voting system. The technology of electronic voting (E-Voting) is used to support the on duty public servants to easily contribute their vote in decision making in a democratic way. E-Voting is an election system that allows a voter record his or her secure and confidential vote [1]. E-Voting is casting a vote electronically by tabulating votes using the Internet. The main goal of a secure e-voting system is to ensure that privacy of the voter's and accuracy of the votes. The authenticating voter's and polling data safety aspects for e-voting systems are discussed here [2].

B. Securities Requirements for E-voting Systems :

A secure e-voting system is satisfying the following requirements:

- Correctness: cast ballot cannot be altered. Therefore, it will not be modify, once the election has been closed.
- Eligibility: Only genuine voters shall be taken an account.
- Un-reusability: Every voter is permitted to cast only one vote.
- Inscrutability: voters, votes are set to be top secret.
- Fairness: partial tabulation of votes is impossible.
- Voter verifiability: Anybody should be capable to readily make sure that validity of the whole voting process.
- Vote and exit: once a voter has casted their vote, no further action will perform and voter is exited.

There are lots of software engineering challenges for developers that are:

- Accuracy: It is not possible for a voter to be changed vote and invalid vote filtered from final list, they cannot eligible for voting.
- Privacy: Neither authority or admin nor anyone else can link any ballot to the voters.
- Democracy: It permits only valid voters to vote and, it ensures that valid voter's vote only once.
- Resistance: No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to avoid voters from voting.
- Verifiability: Independently confirmation of that all votes have been counted correctly.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

- Accessibility: The system perform properly as long as the poll stands anywhere and any voter can have right to use to it from the beginning to the end of the poll at one time.
- Restart ability: The system permit any voter to interrupt the voting process to resume it or restart it while the poll stands the existing elections were done in traditional way, using ballot, ink and tallying the votes later.

C. Modules in an E-Voting System:

In E-Voting system there are some main modules that are:

- Administration
- Verification
- Control
- Voting

These all modules connected to each other and perform their work properly. That are maintain list of eligible voter, identification and verification, declare election date, saving and counting of votes and display final result.

D. Today's voting By Public Servants on Election Duty:

All other public servants appointed on election duty have the option of casting their votes through postal ballot system [4]. For this purpose, they will have to apply to the Returning Officer for issuing Form 12. The District Election Officer/Returning Officer will send sufficient number of Forms 12 to enable for voter and the Polling Officers to apply for Postal Ballot Papers. Voters have to send the application form (Form 12) filled up immediately along with the duplicate copy of the order of appointment and submit it to the Returning Officer. After postal ballot is issued to the Polling Staff, the Returning Officer will make arrangement to facilitate their voting and depositing the ballot paper and the connected papers at the training centers itself, so that voter do not have to post the ballot paper in post offices. For
using this facility is necessary to show EDC (Election Duty Certificate). There may not be sufficient time left for voter to record their votes and return it to the Returning Office before counting time. Applications that are comes from voter

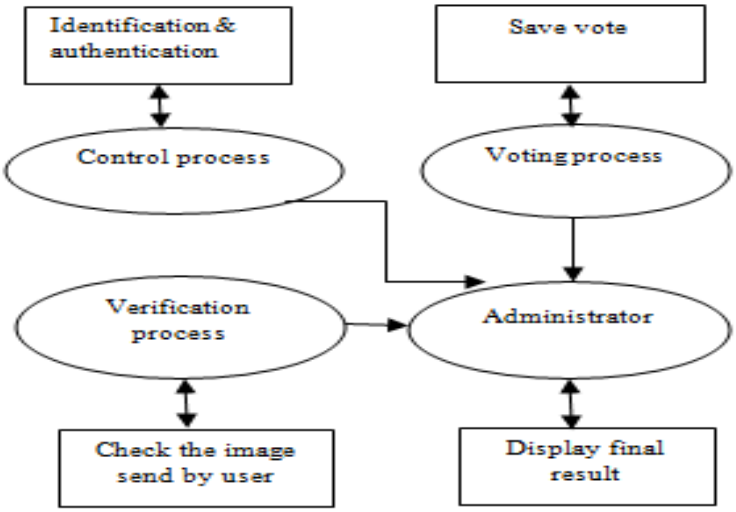


Fig1.1:-A simple block diagram of E-Voting system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

side on election duty to vote by postal ballot are required by law to be made at least seven days or such shorter period as the Returning Officer may allow before the day of poll or the first day of the poll in the constituency.

II. METHODOLOGY

A. Secure information using Cryptography:-

Cryptography is the technique of providing security over transformation of information [8, 11]. From previous days cryptography has been used as a means of providing secure communication between military forces, individuals, and government agencies. Today, cryptography is a keystone of the modern security technologies that is used to protect information and resources on both open and closed networks. Public key cryptography [3] is one of the techniques to protect data in network.

B. Network Security & Cryptography:-

This is an idea to protect network and data transmission over wireless network. The Data Security is the major aspect of secure data transmission over unreliable network. Data Security is a challenging and an important issue of data communications. Today network security touches many areas including strong data encryption technique, secure communication channels, and trust in third party to keep the database. The conventional methods of encryption can only maintain the data security. The very fast development in information technology, that secure transmission of secret data here with gets a huge deal of attention. The information could be accessed by the unauthorized or illegal user for malicious purpose. For that reason, it is necessary to apply effective encryption/decryption methods to improve data security.

For network authentication here we will use Kerberos concept. Kerberos gives a concept over computer network authentication protocol which works on the basis of "tickets" to permit nodes communicating over a non-secure network to confirm their identity to one another in a secure manner.Its designers designed primarily at a client–server model, which provides mutual authentication between both server and the user, verify each other's identity.

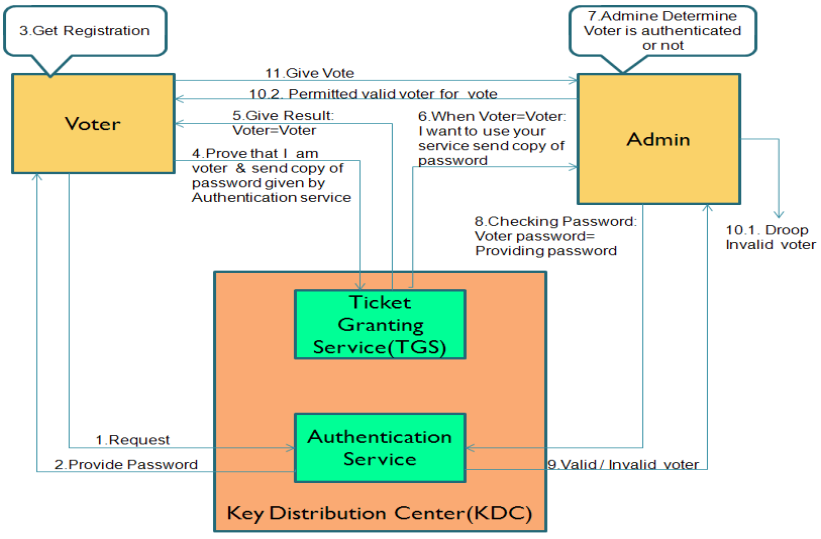


Fig-2.1:-Proposed system architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

The Kerberos protocol messages are protect against repeat and eaves dropping. Kerberos builds on private key cryptography and requires a trust on third party, with optionally use of public-key cryptography [6] during certain phases of authentication. The proposed system architecture is shown in fig-2.1.

III. ALGORITHM USED

A. Proposed Algorithm:

In public-key cryptography, encryption and decryption are done using a pair of keys such that knowledge of one key does not give knowledge of the other key in the pair [7]. One key is published that is called the public key, and the other key is kept as private key. This second key is calledprivate key, and not to be confused with a secret key which is shared by the parties to communication in a conventional cryptosystem. Public-key cryptography has many advantages over conventional cryptography when used for authentication, these will include more natural support for verification to multiple recipients, support for non-repudiation and the removal of secret encryption keys from the central authentication server.

While public-key encryption is method for use in authentication by forward and store applications such as e-mail [1], and it is required by applications where a provided proof is verified by several readers [17],there is a trouble for high-performance servers that perform many authentication operations.

When to add public-key support to Kerberos, then it can be confined to the initial request for a ticket that is , granting ticket, allowing users with registered public keys for privacy enhanced in mail. To get Kerberos tickets for application servers that support Kerberos authentication. For Subsequent exchanges, mainly the application request would apply conventional cryptography for improving performance [7].

The public key in this cryptosystem consists some of the value that are:

m : which is called the modulus,
e : which is called the public exponent.

The private key also consists of some values that are:

m : which is called the modulus
d : which is called the private exponent.

In an RSA algorithm public-key / private-key pair can be generated through the following steps [3]:

1. Create a pair of large, random prime's a and b.
2. Calculate the modulus m as m = ab.
3. Choose an odd public exponent e between 3 and m-1 that is relatively prime to p-1 and q-1.
4. Calculate the private exponent d from e, a and b.
5. Output is (m, e) as the public key and (m, d) as the private key.

The operation of encryption in the RSA cryptosystem is performed with the help of exponentiation to the e^{th} power modulo m:

$O = ENCRYPT (I) = I^e \bmod m.$ (3.1)

Where:

I: Input message;
O: output or resulting cipher text.

In this concept, the message m is normally some type of appropriately formatted key that is to be shared. The original message is encrypted through the shared key using a traditional encryption algorithm. This concept makes it possible to encrypt a message of several lengths with only one exponentiation.

The operation of decryption is performed with the help of exponentiation to the d^{th} power modulo m:

$I = DECRYPT (O) = O^d \bmod m.$ (3.2)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

The connection between the exponent's e and d ensures that encryption and decryption are inverses; therefore the Decryption operation recovers the original message *I*. Without the private key (m, d) (or equivalently the prime factors a and b), it's complicated to recover *I*from *O*. According to this m and e can be made public without compromising security, which is the essential requirement for a public-key cryptosystem.
Main fact is that the encryption and decryption operations are inverses and work on the same set of inputs also means that the operations can be employed in reverse order to obtain a password (p).Applying the decryption operation on to it, i.e., by exponentiation it to the d^{th} power:

$$p = \text{PASSWORD}(I) = I^d \bmod m. \quad (3.3)$$

Then password can be verified by applying the encryption operation to it and match the result with and recovering the message:

$$I = \text{VERIFY}(p) = p^e \bmod m. \quad (3.4)$$

In this concept, the plaintext *I* is normally some function of the message, for instance a format one-way hash of the message. That makes it possible to verify password of any length with only one exponentiation.

B. *Voter Account Maintenance:*
When any voter register him/herself for using e-voting facility then this system verify that voter is valid or not. If voter is valid then creates an account of that voter and activated his/her account for particular election date, Once individual voter passes the authenticity criteria, then he/she will be login into his/her voting account. Admin restrict a voter for logging into his/her voting account only once during that elections date. Once a particular voter is login using password given by the TGS, a secure channel will be established between voter and admin after that, he/she will be able to cast the vote. Votes will remain secret in any condition, i.e., it will not be reflect anywhere in the database, that is which user has voted for whom. Finally, the account will be automatically deactivated and that user will not be able to login back again. This completes the voting process.

IV. RESULT AND DISCUSSION

A. *First step of online voting is to send request to admin for on-line vote, register him/herself and fill the registration form given below:*
In this form voter will fill their details like voter's name, father's name, mother's name, address, gender, date of birth, contact number, mail address, voter ID number, constituency, scan copy of voter photo and voter ID card. There is a filter in date of birth section; if voter is below 18 years then they can't register him/herself and a message "Your Age Is Less than 18 Year!" will display. Shown in figure "A".

B. *Registered Voter's list maintain by administrator is given below:*
After registration a message will be received in voter's e-mail address consisting voter ID and password, login for voting process. And a list maintained by the admin in which all registered voter's detail is recorded.Admin checks the validation of the voters. After verifying process, admin can activate or deactivate particular voter.Shown in figure "B".

C. *Election held on which date is maintain in below page:*
In this page admin set a date which will hold on particular election date. This page is divided into four sections: New Election, Active Election, Postponed Election and Cancel Election.Shown in figure "C".

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

D. *New Election page:*
In this page admin can add new election by inserting name of election and date on which election holds. By clicking add button, the new election is added in the list.Shown in figure "D".

E. *Active Election page:*
In this page, added election is activated. Till the time it is not activated, voters can't vote. Shown in figure "E".

F. *Postpone Election page:*
In postpone election; we have to enter the newly selected date of the same given election.Shown in figure "F".

G. *Cancel Election page:*
Sometime election is cancel due to some reason. For those cases this page is developed. In this page select election name and date then cancel that election.Shown in figure "G".

H. *Change Password page:*
In this page admin can change their password for security purpose. First admin has to enter username "admin" then type old password, after that enter new password and retype same new password for conformation. This process protect from hackers attack.Shown in figure "H".

I. *Voting Page:*
In this page, voter enters through "user ID" and "password." Without this, voter cannot enter in this page. After voting when any voter again login, their Id and password will not allow re-login using same user ID and password. For voting process admin provide 60 seconds (1 minute) time duration for selecting candidate and vote their best candidate. If voter does vote within 60 seconds, it wills automatically logout. Shown in figure "I".

J. *Display Result Page:*
In this page result is display. This page holds information about how many voters are registered for voting process. This page also calculates how many of them are actually give their vote and how many are not voted. This page also displays total votes and it percentage for individual candidate. Shown in figure "J".

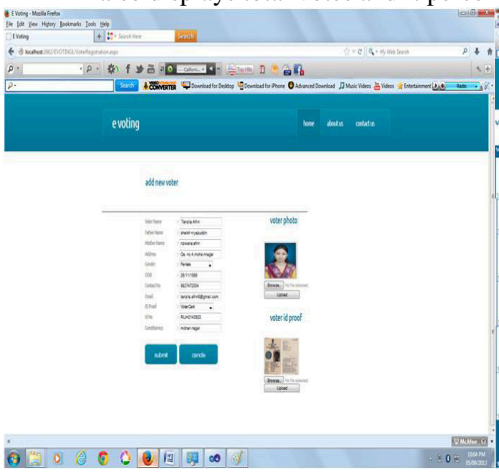


Fig A: Registration Form

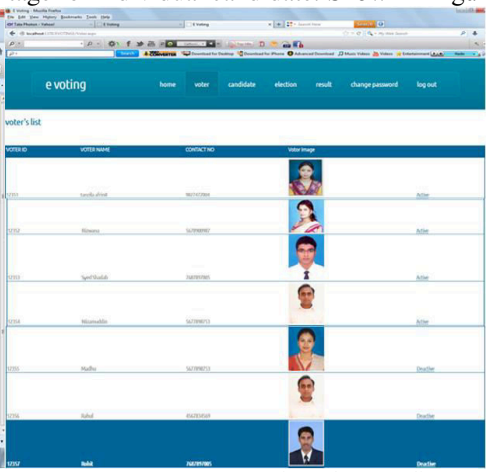


Fig B:-Registered Voter's list

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

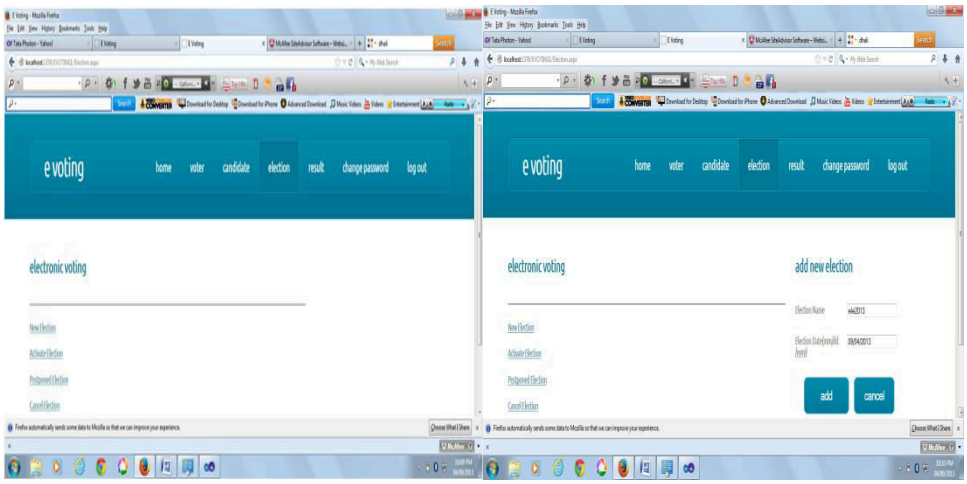


Fig C:-Election date Maintenance Page

Fig D-New Election

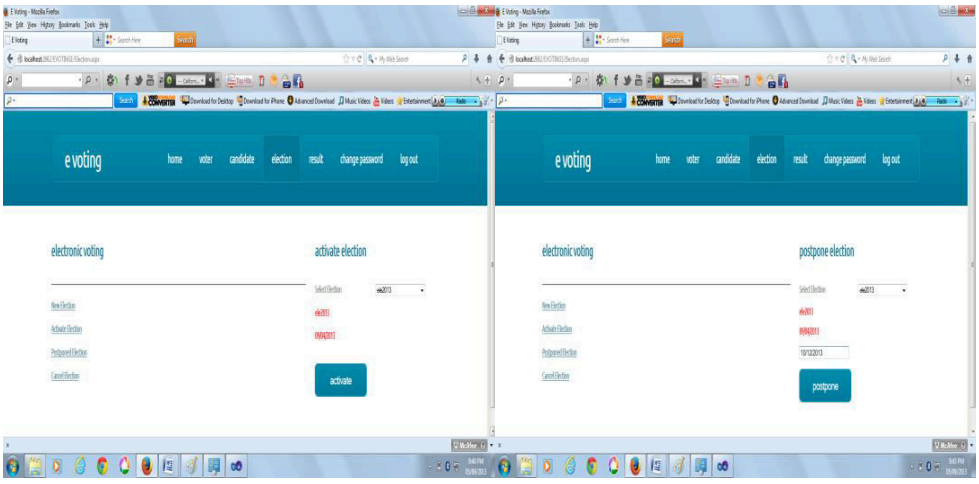


Fig E-Active ElectionFig F-Postpone Election

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

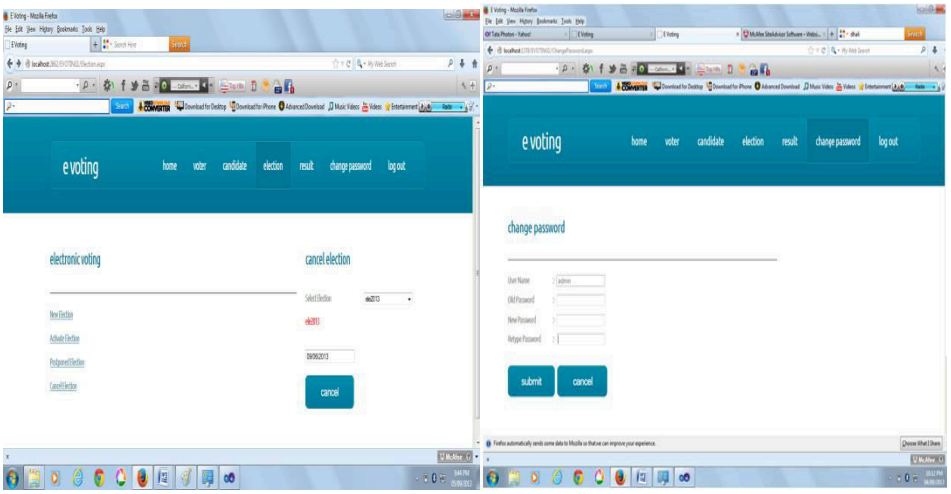


Fig G-Cancel ElectionFig H- Change Password

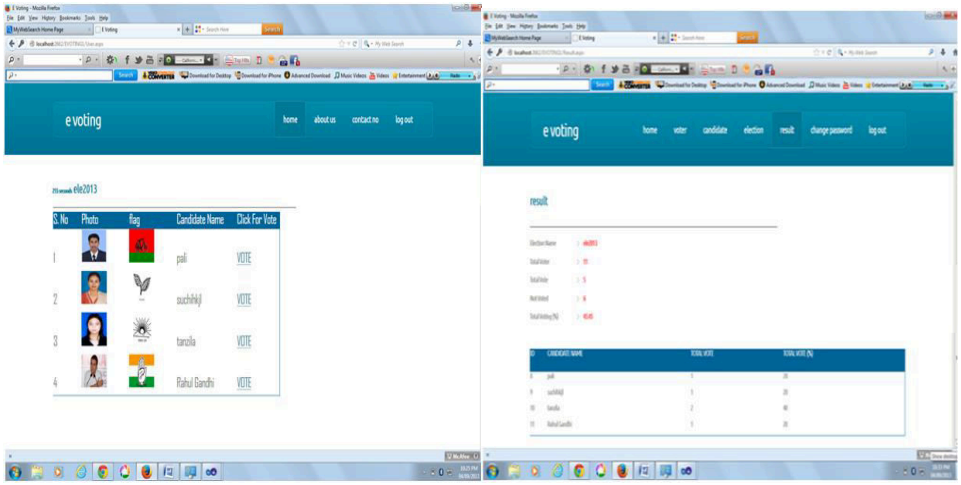


Fig I- Voting pageFig J- Result Display

V. PROPOSED FURTHER RESEARCH WORK

In over contrary there are many types of voter that are general voter, on-duty voter and physically handicapped voter. This system is proposed for on Duty Public Servants to cast their vote easily. Future enhancement of this system is that it will implement for physically handicapped voter, mainly for blind voters. Blind voters give their vote by voice. Addition of voice sensor in this concept is future enhancement.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

VI. CONCLUSION AND FEATURE

The proposed scheme is to make an efficient electronic voting scheme, that provides essential security requirements and the voter's identity remains hidden. It utilizes the advantages of the threshold cryptography to make the counting votes submit to group of authority. The secure internet voting system should not only allow all voters to verify the voting result but also avoid ballot paper issuing. The proposed internet voting system uses threshold verification to protect the content of the ballot during casting, the proposed internet voting system is verifiable and discourages ballot buying at the same time. So our scheme is expected to serve as efficient and secure service.

REFERENCES

1. A.I. Khamg&A.R.Ramli. "Implementation and Evaluation of New Cryptography Algorithm for E-mail Applications", International Journal of the Computer, the Internet and Management Vol. 17.No.1 (January-April, 2009).
2. KomministWeldemariam, Richard A. Kemmerer, Adolfo Villafiorita,"Formal Specification and Analysis of an e-Voting System", 2010 International Conference on Availability, Reliability and Security, 978-0-7695-3965-2/10 $26.00 © 2010 IEEE DOI 10.1109/ARES.2010.83
3. Rasmi P S, Dr. Varghese Paul," An Implementation of a New public key System based on RSA which leads hackers solve multiple hard problems to break the cipher", 978-1-4673-5119-5/12/$31.00 c 2012 IEEE
4. http://eci.nic.in/eci_main/ElectoralLaws/HandBooks/Handbook_for_Presiding_Officers.pdf.
5. XinZhou,Xiaofei Tang," Research and Implementation of RSA Algorithm for Encryption and Decryption", 2011 The 6th International Forum on Strategic Technology 978-1-4577-0399-7/111$26.00 ©20111EEE,August 22-24, 2011.
6. Hayam K. Al-Anie," E-voting protocol based on public-key cryptography", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011
7. W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6):644-654, November 1976.
8. Vishwa Gupta, Gajendra Singh, Ravindra Gupta," Advance cryptography algorithm for improving data security",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 1, January 2012 ISSN: 2277 128X.
9. Ishtiaque Mahmud, Shamim Ahmed, A.K.M NazmusSakib, QuaziEmanualAlendey, IsratJahan, "E-Voting Security Protocol: Analysis & Solution", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012.
10. JaydeepHowlader, Vivek Nair, SaikatBasu and A. K. Mal," Uncoercibility In E-Voting and Eauctioning Mechanisms using Deniable Encryption ", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.
11. Vishwa Gupta, Gajendra Singh, Ravindra Gupta "A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA", International Journal of Computer Science & Communication Networks, Vol 1(3), 258-263, ISSN:2249-5789.
12. Kuldeep Singh, Rajesh Verma, RitikaChehal," Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012.
13. Karlof, N. Sastry, and D. Wagner, (2005), "Cryptographic voting protocols: A Systems perspective", 14th USENIX Security Symposium, pp. 33-49.
14. M. Abo-Rizka, and H. Ghounaim, (2007)" A Novel in E-voting in Egypt", IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.11.
15. T. ElGamal, (1985) "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, IT-31(4), pp. 469–472.
16. DriptoChatterjee, JoyshreeNath, SuvadeepDasgupta, AsokeNath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.
17. Symmetric key cryptography using random key generator, , A.Nath, S.Ghosh, M.A. Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.
18. Data Hiding and Retrieval, A. Nath, S. Das, A. Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.
19. Chum-Ta Li, Min-Shiang Hwang, Yan-Chi Lai, "A Verifiable Electronic Voting Scheme over the Internet", Sixth International Conference on Information Technology: New Generations, 2009.
20. Shobhalokhande,Dipalisawant,NazneenSayyad,MamataYengul," E-Voting through Biometrics and Cryptography- Steganography Technique with conjunction of GSM Modem", Emerging Trends in Computer Science and Information Technology -2012(ETCSIT2012)Proceedings published in International Journal of Computer Applications® (IJCA).
21. William Stallings,"Cryptography and Network Security, Principles and Practices", Third Edition, pp. 67-68 and 317-375, Prentice Hall, 2003.
22. T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an Electronic Voting System," Security and Privacy, IEEE Symposium on, vol. 0, p. 27, 2004.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

23. Deepak Garg, SeemaVermaThapar University, Improvement over Public Key Cryptographic Algorithm, 2009 IEEE International Advance Computing Conference (IACC 2009)Patiala, India, 6-7 March 2009.
24. Baocang, W. and H. Yupu, 2005. Public key cryptosystem based on two cryptographic assumptions. IEE Proc. Communi., 152: 861-865.DOI: 10.1049/ip-com: 20045278.
25. D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. Kemmerer,W. Robertson, F. Valeur, and G. Vigna, "Are Your Votes Really Counted? Testing the Security of Real-world Electronic Voting Systems," in Proceedings of the International Symposium on Software Testing and Analysis (ISSTA), 2008, pp. 237–248.

BIOGRAPHY

Ms.Tanzila Afrin received the B.E. From Pt. *RavishankarShukla University, Raipur* (C.G.), India in Computer Science & Engineering in the year 2008. She is currently pursuing M.Tech. Degree, in Computer Science Engineering with specialization in Software Engineering from CSVTU Bhilai (C.G.), India. She is currently working as Assistant Professor with the Department of Computer Science & Engineering in Chhattisgarh institute of Technology, Rajnandgaon (C.G.), and India. Her research areas include Software Engineering, Cryptography etc.

Prof. K. J. Sataois in Computer Science & Engineering department and Head of Information Technology Department at Rungta College of Engineering & Technology, Bhilai (C.G.),India. He has obtained his M.S. degree in Software Systems from BITS, Pilani(Rajasthan), India in 1991. He has published over 40 Papers in various reputed National & International Journals, Conferences, and Seminars. He is Dean of Computer & Information Technology faculty in Chhattisgarh Swami Vivekanand Technical University, Bhilai, India (A State Government University). He is a member of the Executive Council and the Academic Council of the University. He is a member of CSI and ISTE. He has worked in various Engineering Colleges for over 25 Years and has over 4 Years industrial experience. His area of research includes Operating Systems, Editors & IDEs, Information System Design & Development, Software Engineering, Modeling & Simulation, Operations Research, etc.