International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Internet Voting

Vishal B.Khobragade[1], PriyankaDhasal[2]

[1]Scholar, Department of Information Tech., Patel College of Science & Technology, Ralamandal, Indore India

[2]Professor, H.O.D. Department of Information Tech., Patel College of Science & Technology, Ralamandal, Indore India

Abstract: ***This paper introduces on internet voting system, that have security context or known as e-trusted voting system. In this study, the prototype builds based on secured and trusted framework for internet voting.The System allows the voters to participate by using username and password .Voter can enter the system and votes on the existing text during election date and the voter can see the result after the end of electiondate***

Keyword: RSA, Digital Signature, Mix-Net, Encryption, Decryption

1. Introduction

The Internet is changing citizen expectations around the speed and convenience with which all government services and elections should be delivered. We use the Internet to shop, bank, maintain our social and professional networks, and to find answers to our questions. Since 2004, when Elections BC introduced North America's first fully integrated online voter registration service, British Columbians have also been using the Internet to register to vote. It is natural that citizens are asking when they will be able to vote online, especially given that banking and other transactions requiring security to protect personal information are now routinely performed in the virtual world. Policy makers are looking for ways to meet citizen expectations in terms of convenience and access to government services. Internet voting is currently used by several municipalities in Canada. Questions about Internet voting have sparked a vibrant debate, as policy makers, election administrators, computer experts, academics, private technology suppliers and interested members of the public discuss the potentially far-reaching implications of this form of voting for the security, transparency and integrity of voting and counting processes. Several prominent computer security and e-law experts have expressed concerns about the suitability of the Internet as a voting platform.On the other hand, Internet voting has been used in elections of national-level governments in Estonia, and at smaller scales in several established democracies, including local governments in Canada. Voter has to participate in the counting stage by checking that his vote is listed correctly inthe tallying list, and then sending a part of the votein order to complete voting. In this protocol, verifiability is defined as "No one can falsify the result of the voting".

2. Internet Voting Security

Direct-recording electronic (DRE) voting systems have been widely criticized for various deficiencies and security vulnerabilities: that their software is totally closed and proprietary; that the software undergoes insufficient scrutiny during qualification and certification; that DREs are especially vulnerable to various forms of insider programmer attacks; and that DREs have no voter verified audit trails paper or otherwise that could largely circumvent these problems. All of these criticisms of DREs apply directly to SERVE as well .Because of space constraints; they have mentioned only a few of the possible attacks. These attacks depend on fundamental vulnerabilities in the current PC architecture for example, malicious code and in the Internet (such as spoofing and denial-of service attacks). These attacks can be launched by anyone in the world, and in many cases may be successful while remaining completely undetected. Consequently, they conclude that Internet voting in general and SERVE in particular, cannot be made secure for use in real elections for the foreseeable future.

3. Analysis of the E-Voting

E-voting has been used in Europe, for legally binding elections, since at least 1982 .Its use is still not widespread, though interest has increased. The Netherlands was a very early adopter, and it was almost a decade later (1991) that Belgium started experimenting with e-voting. Just a few years later, in the mid-nineties, France did the same. By the early 2000's, experiments or pilots had been run in the United Kingdom, Italy, Spain and the Republic of Ireland , among others. In the absence of controversy, surveys of voter attitudes usually reflect satisfaction and trust .When concerns are raised by experts and in the media, however, public opinion can change dramatically. For example: in Ireland in 2003 a survey by Amarach Consulting found that a majority of Irish citizens were in favor of the introduction of e-voting. Less than a year later, after controversy over the system had led to the establishment of the Commission on Electronic Voting, a Red C survey found that 58% of respondents felt that ". . . the e-voting proposal should be scrapped until such time as a paper backup is incorporated into the system . . ." and "one third of all voters were unconvinced that their choices will be registered properly". This instinctive trust of e-voting systems also appears to exist amongst officials. When government representatives speak about e-voting it tends to be in very positive terms. Their statements emphasize the benefits of e-voting; the largest obstacle, from their point of view, is usually gaining the voters' trust. The idea that the system in question might not deserve such trust is given little or no attention, except where it overlaps with "allaying public concern" about the security of the system. Two prime examples of this are the web pages for the voting systems of the Irish Government and the Swiss state of Geneva. In reality, implementing e-

voting is not so simple identified one of the most significant obstacles – the conflict between the requirements for secrecy and accuracy. Serious problems also arise from the way in which voting systems are currently developed. To knowledge there is still no voting system that has been treated as safety-critical in its development and deployment . These and other factors have combined to create serious issues in legally binding elections. Examples of worrying incidents in real elections in the US have been gathered by the Verified Voting Foundation's Election Incident Reporting System.

4. Security Threats

When vote is travelling from voter i.e. voting client to voting server, there are some security threats to that casted vote.

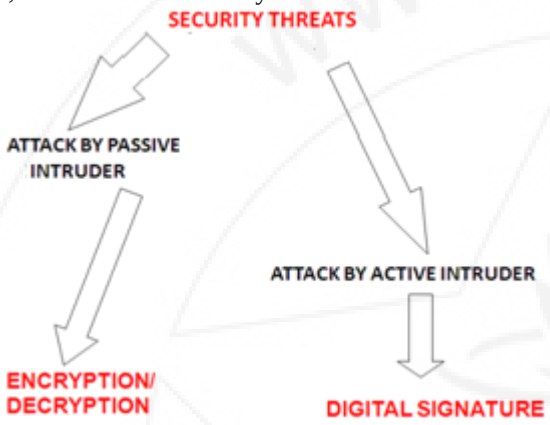

Figure 5.2: Security threats to Internet voting system

These security threats includes attacks by intruder, there are two types of intruder Passive intruder and Active intruder. **Passive intruder** access the unauthorized data, when data is in transmission condition and use for destructive use. To provide security from such intruder we use cryptographic approach. **Active intruder** access the unauthorized data, when data is in transmission condition and make some changes in that data again send that changed data to receiver. Due to this receiver get corrupted data.

5. Homomorphic Encryption Models

A number of protocols have been proposed which conform to methods of holomorphic encryption. The first scheme using holomorphic encryption had been proposed by Benaloh and Yung. Further modification to this model was carried out by Sako and Kilian to improve communication efficiency. Thereafter the model proposed by Cramer, Gennaro and Schoen makers which was a relatively simple and efficient scheme. Benaloh and Tuinstra introduced concept of receipt freeness which was later disproved. In this model, the voter sends his encrypted vote through a public channel. The vote can be decrypted by any set of at least "t + 1" authorities, and any set of the "t" authorities cannot decrypt the encrypted vote.

This model can be implemented in two ways:

- A key to decrypt the vote is shared between any set of "t + 1" authorities which is known as threshold public-key cryptosystem, as in ElGamal cryptosystem.
- Each authority has its own instance of the cryptosystem. The voter shares his encrypted vote among the N authorities using (t+1, N) secret sharing scheme .The voter sends to the each authority its encrypted share. This will prevent malicious authorities to abuse their role and to violate voter's privacy. Encryption method used for encrypting votes is homomorphic, i.e. Multiplication of the encrypted votes v1,v2: E(v1) ⊗E(v2) is an encrypted sum of the votes E(v1⊕ v2). In a yes/no voting, votes are represented by +1 for yes and -1 for no. Let be p and q be large primes such that q is a factor of p-1 and let g Є Zp be an element of order q. The secret encryption key is x Є Zq and the public encryption key is $y = g^x \bmod p$, *and* $w=y^kg^v \bmod p$, where k is a random number in Zp .(Z,p) is decrypted by taking w/Z^xmodp and by comparing the result with g modp and g^-1 modp .Each voter encrypts his/her vote with the public encryption key of a voting authority and then publishes the encryption on a bulletin board, together with a proof of correctness: that the encryption contains a valid vote At the end of the voting period the authorities "multiply" all the received encryptions to get an encryption of the tally. The authorities then jointly decrypt this. The final tally can be checked for accuracy by all parties. So we are assured of universal verifiability. For robustness the encryption procedure is distributed among n authorities using threshold cryptography. An election system based on the Cramer et al scheme [8] has been implemented and piloted on a limited basis. A drawback of such schemes is their reduced flexibility, as the votes are essentially limited to yes/no value. In addition, the Cramer et al scheme which uses ElGamal encryption has a relatively high computational complexity, if the number of candidates is large. Alternative homomorphic encryption voting schemes have been proposed for which the computational complexity is either linear, or even logarithmic.

6. Schemes Based on Mixed-Nets

The initial schemes based on mixed nets were devised by David Chaum. The mix-net model is composed of several linked servers where each server accepts a batch of encrypted votes randomizes it and then outputs a batch of permuted votes such that the input is unlinkable with the output vote. First the authority takes the batch of encrypted votes, permutes it in a random order, and then re-encrypts each encrypted vote. The permutation is known only to the voter. The permutated batch of re-encrypted votes is published and handed to the next authority; unless the permutation is unveiled to a person no one can map the original vote to the new permuted vote.

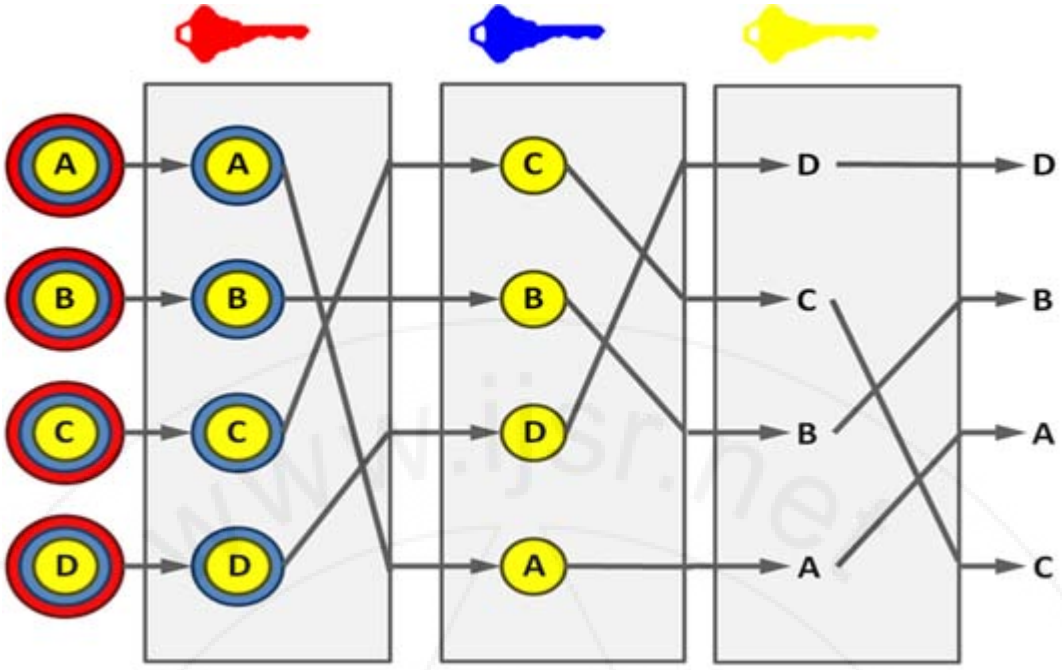

Fig 4.1 A general Mix-net model The next authority shuffles the votes in the same way as the first authority shuffled the original batch: it permutes the batch in a random order, re-encrypts each vote, and unveils the permutation to the voter publishes the produced batch of votes. This process is repeated for several times, in the final stage the last authority performs the same process and publishes the final list of permuted and re-encrypted votes. Therefore, only he knows the voter can map his vote in the final list of the permuted votes. In large-scale elections, this model of mixed nets is useful because of their universal verifiability, anonymity property.

7. Our Security Approach

In our proposed system, voting server has a pair of asymmetric key to provide security from passive intruder. Each registered voter has a pair of asymmetric key to provide security from Active intruder.

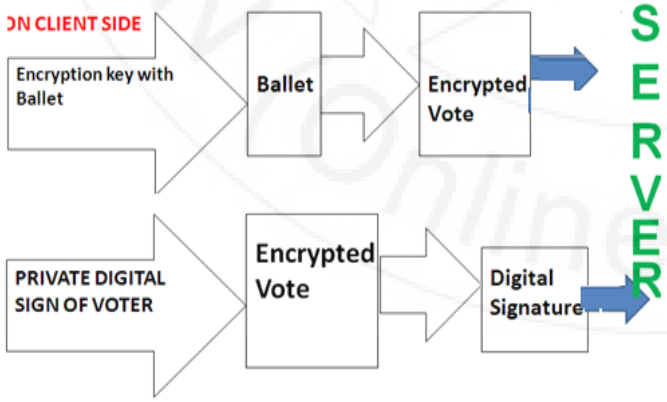

Figure 5.4: voting Client side computing.

The vote is encrypted by public encryption key provided with ballet when voting is done. And decryption is done by private decryption key of voting server when counting is done.Here encryption is done by public key which publicly available and decryption is done private key which is private. To provide security from such intruder we are using the concept of Digital Signature.

As above figure shows processing on VOTING CLIENT side,

1) When voter go for voting first he/she request for Ballet. As reply server sends Ballet along with public encryption key of system for encryption of casted vote.
2) When voter cast his/her vote that casted vote is encrypted by system public encryption key.
3) There after voter again encrypt (digitally sign) that already encrypted vote by using his/her private encryption key.
4) Voter sends both casted encrypted vote and output of second time encryption using voter private key (digital signature) to the server.

8. On Sever Side

Sever checks digital signature of voter using voter public decryption key. If signature is valid casted vote is stored for counting otherwise ERROR massage is sent to voter

References

[1] Ali FawziNajm Al-Shammari, Sergio Tessaris" Vote Verification through Open Standard: A Roadmap", 978-1-4577-0953-1/11IEEE2011.
[2] Amir Omidi and Mohammad AbdollahiAzgomi, "An Architecture for E-Voting Systems Based on Dependable Web Services" 978-1-4244-5700-7/10 ©2009 IEEE
[3] Amir Omidi,SaeedMoradi "Modeling and Quantitative Evaluation of an InternetVoting System Based on Dependable WebServices", 978-1-4673-0479-5/12/©2012 IEEE
[4] Haijun Pan, Edwin Hou and Nirwan Ansari" Ensuring Voters and Candidates' Confidentiality in E-voting Systems" 978-1-61284-680-4/11/$26.00 ©2011 IEEE
[5] Seo-Il Kang and Im-Yeong Lee "A Study on the Electronic Voting System using blind Signature for

Anonymity", IEEE 2006 International Conference on Hybrid Information Technology (ICHIT'06) 0-7695-2674-8/06

[6] Chun-Ta Li, Min-ShiangHwang , Yan-Chi Lai "A Verifiable Electronic Voting Scheme Over the Internet", 2009 Sixth International Conference on Information Technology: New Generations

[7] LazarosKyrillidis, Sheila Cobourne, Keith Mayes, Song Dongy and KonstantinosMarkantonakis" Distributed e-Voting using the Smart Card Web Server" 978-1-4673-3089-3/12@ 2012 IEEE

[8] Y ousfiSouheib, DerrodeStephane, "Watermarking in e-voting for large scale election", 978-1-4673-1520-3/12/$31.00 ©2012 IEEE

[9] AnkitAnand, PallaviDivya, " An Efficient Online Voting System", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.4, July-Aug. 2012 pp-2631-2634

[10] Dr. ShaliniVermani, Dr.NeetuSardana, "Innovative Way of Internet Voting: Secure On-line Vote", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012 ISSN (Online): 1694-0814

[11] "An Efficient Implementation of Electronic Election System" by NazninFauzia ,TanimaDey ,InabaBhuiyan ,Md. SaidurRahman.

[12] "A Critical View on Internet Voting Technology", EleniTsekmezoglou, John Iliadis

[13] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S.Wallach."Analysis of an electronic voting system."In IEEE Symposium on Security and Privacy, May 2004.

[14] ZuzanaRjašková ," Electronic Voting Schemes Diplomovápráca", ,April 2002

[15] David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, 24(2):84–88, 1981.

[16] "An Analysis of Chaum's Voter-Verifiable Election Scheme" , Julie Ann Staub, Master of Science, University of Maryland, College Park, 2005

[17] Josh Cohen Benaloh and Dwight Tuinstra."receipt-free secret-ballot elections ", Proc. 26th ACM Symposium on the Theory of Computing (STOCK), 1994.

[18] Josh Cohen Benaloh and Moti Yung. "Distributing the power of the governement to enhance the privacy of voters",1986.