The Design of Web Based Secure Internet Voting System for Corporate Election

Jagdish B. Chakole[1], P. R. Pardhi[2]

[1]Deptt. of Computer Science & Engineering, R.C.O.E.M.,
Nagpur, Maharashtra (India)

[2]Deptt. of Computer Science & Engineering, R.C.O.E.M.,
Nagpur, Maharashtra (India)

Abstract: ***In a traditional voting environment voting process sometimes becomes quite inconvenient due to the reluctance of certain voters to visit a polling booth to cast votes besides involving huge social and human resources. The development of computer networks and elaboration of cryptographic techniques facilitate the implementation of internet voting. In this paper we propose a secure internet voting system that is suitable for voting over the internet. The proposed voting system is based on digital signatures and cryptography approach and the system will be suitable for corporate company having their offices in different cities. The proposed system encompasses three distinct phases - that of registration phase, authentication phase voting phase and counting phase involving parties, the voter, voting server and voting authority.***

Keywords: Web server, digital signature, internet voting

1. Introduction

Election and voting are all now well known terms in modern days of Democracy. Electronic online voting over the Internet would be much more profitable. Many voters would appreciate the possibility of voting from anywhere. A company having their offices in different locations, can use internet voting for their election, in their employees from all offices will take part in election from their own offices. Electronic voting, as the name implies, is the voting process held over electronic media, i.e. computers. In general, such internet voting system should satisfy such requirements as follows:

1. Accuracy
2. Simplicity
3. Democracy
4. Verifiability
5. Privacy
6. Security.

For such an internet voting system, security and privacy are main concerns. From that point of view, an implementation of secure Internet voting system appears to be another application of cryptography and network security. Electronic voting has been intensively studied for over the last twenty years. Many e-voting system, therefore, have been proposed in the last several decades and both the security as well as the effectiveness has been improved. Nevertheless, to the best of our knowledge, no practical and complete solution has been found for large scale elections over a network, say Internet.

Our approach suggests a practical application of the existing cryptographic schemes and digital signature that ensures integrity of the vote cast by voter and authentication of voter at the two levels. Design of secure e-voting system over a network is indeed a very difficult task as all the requirements of the voting system have to be met. Failure to ensure even one of the specifications can lead to chinks and glitches that can be exploited by a middleman to forge or manipulate the intricate details. Subsequently, the result of the election is computed from the sum of the votes which is jointly decrypted by the authorities. A voting scheme must ensure that the voter can keep his vote private.

2. Literature Survey

This paper [1], review that currently deployed vote verification methods. By discuss their weaknesses with the aim of proposing a more reliable and robust vote verification method. Authors in this paper, sought to propose a vote verification technique which would able to verify vote against major possible threats and enables all election participants to verify votes. For this purpose, they need to investigate a combination of both technological and procedural solutions.

Author [2] proposed design for e voting systems based on dependable web services. The results got from the analysis of the evaluation of the proposed design, presented that solution, increase the dependability to a great extent. Also explained that this design can respond to main requirements of e-voting. The availability is one of key attributes and the most important requirement for e-voting as important as security, which is fulfilled. Considering that the security is a very important requirement of e-voting systems, author has used the existing solutions to achieve web service security. Author of paper [3], proposed architecture for internet voting system based on dependable web services. Then he modeled this system with RBD and Reward Petri Nets. Finally he evaluated these models quantitatively. Also by looking at the results of evaluation, he can decide to use or not to use this system. We can see that his architecture increased dependability very much. Also he considered main requirements of voting like secrecy, mobility, accuracy, uniqueness and etc. Paying attention to security needs of voting, he used some approaches to create a secure system. He showed that this system will not fail even if some components fail and both availability and security as the

most important specification of voting systems will be addressed. As voting via internet is very easy and has no time and money costs for voters. So, systems can anchorage people to take part in the election.

Author [4] proposed an E-voting procedure which ensures voters and candidate's confidentiality and accuracy. Many issues still exist, for example, when large number of voters cast their ballots at the same time, will it cause denial of service (DOS) in the Internet? How to design an efficient and secure online voting system? Nevertheless, at least for the counting procedure, different levels of measurements introduced in our proposal have decreased the risk for unfairness in actual elections.

The proposed deign in paper [5] contains that the voting can be done only at the places where the voting places are installed. Though voting can be done using mobile terminals at any places if the wireless network develops further in the forthcoming days, the additional requirements for security will be required depending on the wireless circumstances. And the way of authentication must be provided more strongly and there should not be coercive voting or exposure of data in the wireless network. Voting is a key way of democracy reflecting the nation's intention. Therefore, a study on security technology applied to the electronic voting system should be progressed continuously in the future.

Author [6] proposed an internet voting protocol. The proposed internet voting protocol adopts blind signature to protect the content of the ballot during casting. As we believe that a secure electronic voting system do not only allow all voters to verify the voting result but also avoid ballot buying, the proposed internet voting protocol is verifiable and discourages ballot buying at the same time. Any unauthorized candidate or party can still try to buy ballots during the election. However, no voter can prove which ballot was cast by him/her after the declaration of the election result. In other words, ballot buying may still exist, but the ballot buyer cannot be assured that the voter will mark the ballot as the buyer want.

3. Participants and Phases

The participants are voter, voting client, voting server, voting authority. The system will be comprised of

Following phases

1. Registration
2. Authentication
3. Voting
4. Counting

Registration phase: A authorize person of organization will go to each office of the company and after verifying valid identity of a employee, will register him/her for voting and give him/her PASSWORD and USERNAME. The voter later can change his/her PASSWORD online for security purpose just like we do when we get ATM card and PIN from bank first time.

Authentication phase: When voter login using username and password, the voting system will check authentication of the voter.

Voting phase: In this phase first request for ballet is done. Voter will get ballet and public encryption key. The vote will encrypt using this key. Again that encrypted vote is digitally sign using voter private key. Encrypted vote and digital signature is sent to voting server. Voting server first check digital signature and then store that encrypted vote.

Counting phase: In this phase all encrypted votes first decrypted and then counting is done. The authorize person will enter the private decryption key for decryption. The counting is done and result will be declared.

4. System Architecture

We are designing this system for an organization having their offices in different cities. Our main concern is that to provide security to casted vote, when it is travelling from voter to voting server for storing, we are focusing to provide security from intruders both passive as well as active. The passive intruder can access the casted vote of a voter and create challenge to secrecy and privacy characteristics of voting system. The active intruder may tamper the casted vote and encounter problem for integrity of casted vote. So to tackle this security concern, we are using the concept of cryptography and taking advantages of digital signature. To provide security from passive intruders, we are encrypting the casted vote on client system, and then will send that to voting server with the help of internet, on server side decryption of that vote is done before counting. We require two keys for this purpose one for encryption on voter system, which should be publicly known and second key for decryption of encrypted vote before counting on voting server, this key must be private. So for this purpose we need a pair of asymmetric keys.

To provide security from active intruder who can alter or tamper the casted vote when vote is transferring from voter to voting server, we are using digital signature. When a voter cast his/her vote after that he/she will digitally sign on that by using his/her own private digital signature, and send this to voting server, on voting server side that signature is checked by digital signature verifier of that voter which is publicly known. For this purpose each voter should have a private digital signature and a public digital signature verifier, for this we are using a pair of asymmetric keys for each registered voter. As figure 1

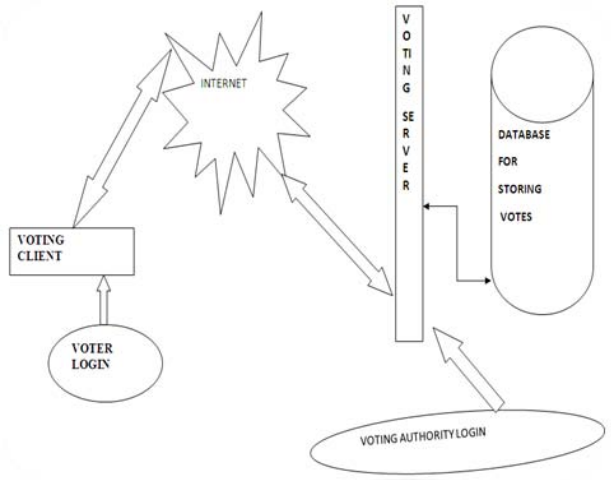

Figure 1: Design of Web based internet voting System Consist of voting sever, voting client, voter and voting authority. A registered voter connects to voting server by using his login identification and password. Voting client and voting server communicate by internet.

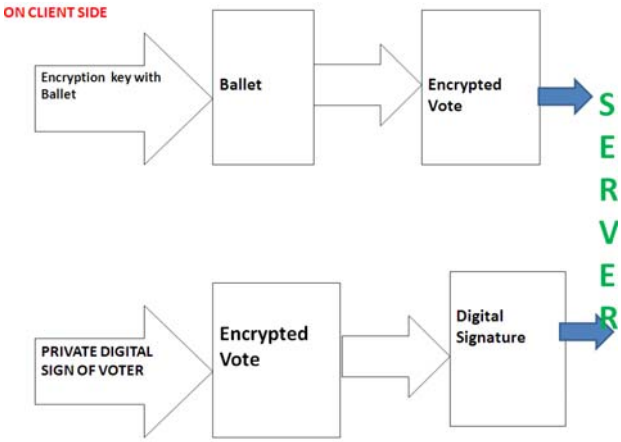

Figure 2: Voting Client side computing

As figure 2 shows computation on client side, when a voter wish to cast vote he first request for ballet to server, server send ballet with public encryption key. Voter encrypts casted vote using this key, then voter digitally sign on encrypted vote by using his private key. And send both to the server.

On server side, voting server verifies digital signature of voter by applying decryption on voter signature using public signature verifier of voter. If signature is valid vote is store for counting otherwise vote is discarded.

5. Results and Implementation

The authorized voting authority will visit to each office of company and do registration of voter by manually verifying the identification of employee. During registration voter generate a pair of asymmetric keys in which one is private and other is public voter keep his private key secrete and other public key goes to server along with other registration details of voter.

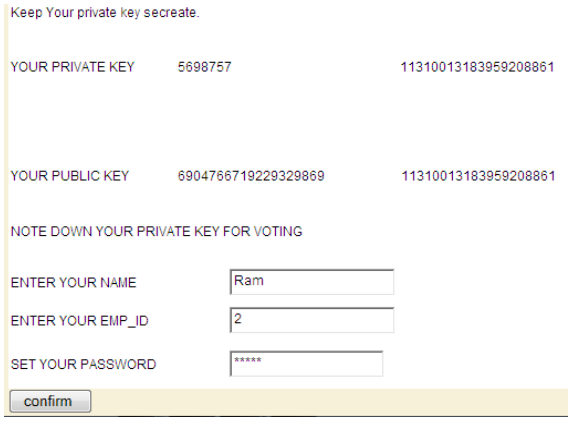

Figure 3: screen showing voter registration form

For security purpose voter can change his/her password by login on the website.

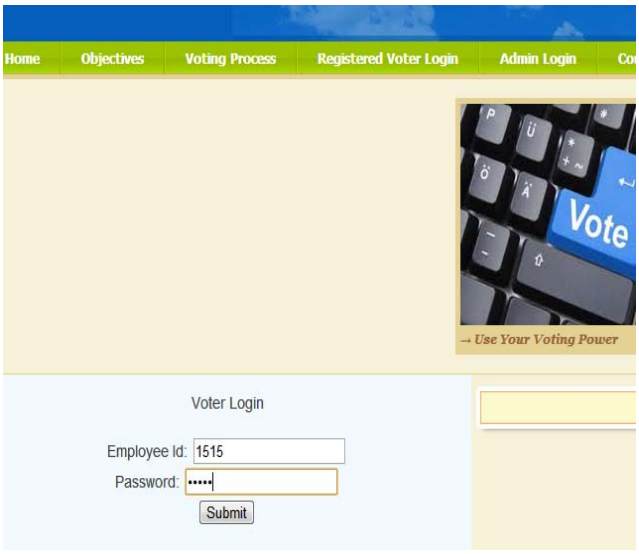

Figure 4: Voter Login Form

On the day of election voter login using own username and password. When voter request for ballet, server send ballet along with public encryption key. Voter cast his vote and encrypts it using public encryption key.

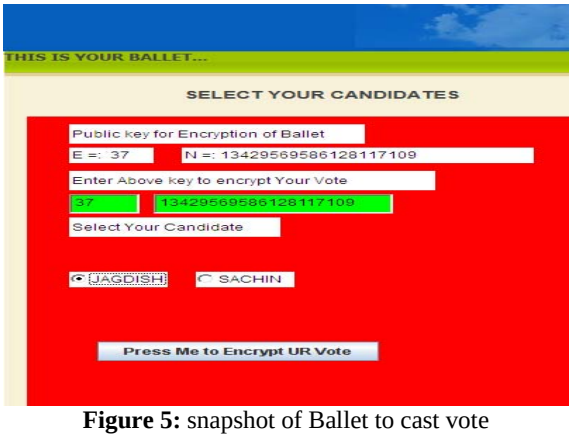

Figure 5: snapshot of Ballet to cast vote

We have internally assigned an Id with each candidate competing for election when voter cast his vote that Id is encrypted by public encryption key provided with ballet.

After that voter digitally sign on that vote using own private digital signature. And send both these to server.

Figure 6: snapshot of Ballet after encryption and digital signature

If the casted vote is access by passive intruder, he cannot know to whom voter has voted because vote is in encrypted form. If active intruder altered the vote and send it to voting server, server easily knows about alteration of vote because vote digitally signed, active intruder alter vote signature also altered and server when verifies signature, server came to know that vote altered and server inform voter about it.

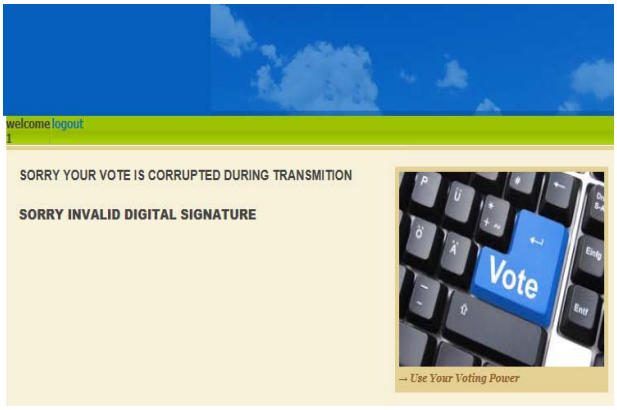

Figure 7: snapshot of corrupted vote i.e. invalid digital signature

After election is voter, on the day of counting authorize voting officer, decrypt the encrypted vote to normal vote by using private decryption of voting system and counting is done and result is declared.

6. Conclusion

We have done experimentation on our system and from that we conclude that this system provide security from all type of attacks, when vote is travelling from voting client to voting server. These attacks include security threats from passive as well as active intruder. We can use this system also for taking opinion of employee on certain issue. In future, for authentication of voter instead of USERNAME, if we can use thumb impression of voter or capture photo of his/her face and compare it with photo stored in our database, it will be more secure. This system saves money, time requirement in traditional voting system. Also it is eco friendly and avoids wastage of paper.

References

[1] Ali Fawzi Najm Al-Shammari, Sergio Tessaris" Vote Verification through Open Standard: A Roadmap", 978-1-4577-0953-1/11IEEE2011.

[2] Amir Omidi and Mohammad Abdollahi Azgomi, "An Architecture for E-Voting Systems Based on Dependable Web Services" 978-1-4244-5700-7/10 ©2009 IEEE

[3] Amir Omidi, Saeed Moradi "Modeling and Quantitative Evaluation of an InternetVoting System Based on Dependable

[4] Web Services", 978-1-4673-0479-5/12/©2012 IEEE

[5] 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

[6] 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

[7] Chun-Ta Li, Min-Shiang Hwang, Yan-Chi Lai "A Verifiable Electronic vote Scheme, 2009 Sixth International Conference on Information Technology: New Generations

[8] Lazaros Kyrillidis, Sheila Cobourne, Keith Mayes, Song Dongy and Konstantinos Markantonakis" Distributed e-Voting using the Smart Card Web Server" 978-1-4673-3089-3/12@ 2012 IEEE

[9] Y ousfi Souheib, Derrode Stephane, "Watermarking in e-voting for large scale election", 978-1-4673-1520-3/12/$31.00 ©2012 IEEE

Author Profile

Jagdish B. Chakole received his B.E. degree in computer engineering from Umrer College of engineering, R.T.M. Nagpur University, Nagpur (M.S.) India, in 2008, pursuing M.Tech. Degree in Computer Science and Engineering from Ramdeobaba college engineering and management Nagpur (M.S.) India. He was a lecturer with Department of Computer Engineering, Umrer College of engineering, R.T.M. Nagpur University, Nagpur (M.S.) India, in 2008, 2009 and 2010 respectively. He taught computer network, system programming, principle of compiler design and internet and java programming to undergraduate student.

Praful R. Pardhi received his B.E. degree in computer science & engineering from V.Y.W.S. College of engineering, Amravati University, Amravati (M.S.) India, in 2001, the M.E. degree in computer science and engineering from M.G.M.'s College of engineering, SRTMU, University Nanded. (M.S) India. He was a lecturer with Department of Computer Science & Engineering, BNCOE, pusad, & JDIET, Yavatmal, Amravati University, Amravati (M.S.) India, in 2001 to 2002, and 2002 to 2007 respectively. He is currently working as a Assistant Professor with Department of Computer Science & Engineering, Shri Ramdeobaba College Of Engineering & Management, R. T. M. University, Nagpur since 2007. He taught Advanced Computer Architecture, Cryptography to postgraduate student and Digital logic design, Computer Architecture Organization, System

Software & Advanced Microprocessor interfacing to undergraduate students. His research interests include digital image processing, computer network security & parallel processing.