A Review on Security Concerns on Internet Voting

[1]Jagdish B. Chakole, [2]P. R. Pardhi
[1,2]Dept. of CSE, RCOEM., Nagpur, Maharashtra, India

Abstract
Nowadays each and every manual system is converting in computerize form which increases efficiency and reduce response time. Voting system is also taking advantages of computerization, now it is a time to take advantages of Internet for voting.
In our proposed system, we are interested in secure online internet voting, for availability we will use redundancy of components of the system. For security and confidentiality we will be interested in digital signature and cryptography.

Keywords
Online Internet Voting, Authentication Server, Counting Server, Mixnet

I. Introduction

In the real world, private information protection is a very crucial task in occasions such as anonymous voting systems and anonymous payment systems. In a true democracy, the constitution grants every citizen the right to vote. Accordingly, every voter can select the right officials for the country. Conventional paper-based voting system is inconvenient for voters and therefore is responsible for decreasing the rate of voting. The main reason is that all legal voters, especially students or businessmen, do not live in their domiciled homes, and each may relinquish their voting right because of the geographical restrictions. The electronic election is a practicable alternative on account of the swift computer network and the benefits from cryptographic techniques. Every voter can participate in the election over the Internet, eliminating the geographical restrictions and thus increasing the rate of voting.
The main goal of a secure electronic voting system is to ensure the privacy of the voters and the accuracy of votes. In general, a secure electronic voting system should satisfy such requirements as follows:

A. Accuracy

A secure electronic voting system must prevent the cast ballot from being altered, duplicated, or removed by anyone. Each legitimate ballot must be count correctly. Furthermore, the possibility must be absolutely eliminated for anyone to forge an illegitimate ballot to cast.

B. Simplicity

The voting process should be as simple as possible. In other words, a user-friendly electronic election interface does not need to learn complex techniques and either additional equipment.

C. Democracy

Only legitimate voters can cast their ballots. Each voter can cast at most one ballot in an election.

D. Verifiability

Each legitimate voter should be able to verify the validity of the cast ballot. Each voter must be allowed to check whether her/his ballot has counted. As the same time, the election result should be verifiable by everyone. The verifiability requirement can be viewed as a means to assure correctness.

E. Privacy

In order to achieve anonymous electronic election, anyone besides the voter her-/himself cannot link to a specific voter when he/she is going through the voting procedure. Private information protection is one of the most important requirements in electronic voting systems.

F. Uncoercibility

Each voter must be able to cast the vote according to her/his own conscience and no voter can be forced to vote in a particular way thanks to the prevention of ballot buying and extortion.
Voting is a very hard and tiring process, since the voters should individually go to voting places. This will decrease the rate of attendance of people in elections. Voting through mail can be suitable, especially for those who live or work in faraway places. Still, this method is time consuming and difficult, because the casting ballots, gathering and tallying the votes are done manually. Internet voting or e-voting can solve this problem. The existing studies have pointed out that e-voting will increase the public attendance in election. As the number of service-oriented applications is increasing, the importance of dependability of them increases, too. Service failure or destruction in these systems can lead to catastrophic consequences. So far, several ways of fault tolerance have been presented; however, this seems to be a vital need for an efficient architecture in the field of dependable web services. Web services, due to their advantages, may have a key impact in usage and deployment of e-voting systems. However, employment of web services faces some major dependability and security issues.
Vote verification is one of the ways to allow such verification by attempting to ensure that cast votes match with voters' selections. We can find two types of vote verification approaches: individual and universal verifiability. Their ultimate goal is a system where any voter (or interested party) without any special training should easily convince herself that the counted vote indeed reflects the actual selection. More specifically, the individual verification allows voters to check if their votes have been properly counted; universal verifiability, by contrast, is achieved when any interested party can verify that the calculated result is correct. A properly designed vote verification method can allow a voter to perform end-to-end verification —namely, allowing checks indicating that votes have been recorded as cast and counted as recorded. It can help discovering whether some malicious attempts have been made to compromise the integrity of election result by providing evidences to election participating entities —such as, voter, electoral staff, and others. Furthermore, many argue that vote verification can increase the trust level of the voting system. In line with this, a number of ongoing works focus on the design and implementation of vote verification methods that can be used during and/or after closing election (e.g., during vote transmission, vote tallying). The majority of these efforts aim at providing technological solutions; most of them are proprietary. For example, most of the voting machines that are currently deployed in polling
Places equipped with special devices in order to provide evidence about cast vote, such as by providing paper audit trail and audio messages.

II. Literature Survey

A paper [1], proposed an electronic voting protocol. The proposed electronic voting protocol adopts blind signature to protect the content of the ballot during casting. Because we believe that a secure electronic voting system should not only allow all voters to verify the voting result but also avoid ballot buying, the proposed electronic voting protocol is verifiable and discourages ballot buying at the same time. Any malicious candidate or party can still try to buy ballots during the election. However, no voter can prove exactly which ballot was cast by him/her after the announcement 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 wishes.

A paper [2], proposed architecture for e voting systems based on dependable web services. The results obtained from the analysis of the evaluation of the proposed architecture, presented that the solution, increases the dependability to a great extent. Also, we explained that this architecture can respond to main requirements of e-voting. The availability is one of these attributes and the most important requirement for e-voting as important as security, which is fulfilled. Considering the fact that the security is a very important attribute of e-voting systems, we have used the existing solutions to achieve web service security.

The proposed method in paper [4] describes that the voting can be made only at the places where the voting places are installed. Though the voting can be made thru mobile terminals at any places if the wireless network develops further in the forthcoming days, the additional requirements for security will be necessary depending on the wireless circumstances. And the way of authentication should be provided more strongly and there should not be coercive voting or exposure of data in the wireless network. Voting is very important 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.

A paper [5] proposed a novel E-voting procedure which ensures voters and candidates' confidentiality and accuracy. Many issues still exist, for example, when millions of voters cast their ballots at the same time, will it cause denial of service (DOS) in the Internet? How to setup 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.

A paper [6], proposed architecture for internet voting system based on dependable web services. Then we modeled this system with RBD and Reward Petri Nets. Finally we evaluated these models quantitatively. Also by looking at the results of evaluation, we can decide to use or not to use this system. You can see that our architecture increased dependability very much. Also we considered main requirements of voting like secrecy, mobility, accuracy, uniqueness and etc. Paying attention to security needs of voting, we used some approaches to create a secure system. We 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 we know, voting via internet is very easy and has no time and money costs for voters. So this system will persuade people to take part in the election.

A paper [7], proposed an overview of an electronic voting system resistant to coercion. This system can be more robust and less expensive if we use technique of watermarking. Adding an imperceptible mark, does not interfere with the talliers during the computation phase of the Ballots. Watermarking could be interesting for the evolution of this system and solve the problem of its complexity.

A watermarking method includes the components of digital communication, signal processing and cryptography. The watermarking method is a technique of dissuasion: The security is to prevent potential coercers that the Ballots are watermarked, so that they may be discouraged from attempting to coerce voters. Steganography does not protect a digital objects, it only ensures their safety in the dark. Nevertheless, the use of a secure cryptosystem and robust cryptographic primitives to ensure the security properties of electronic voting, may make the use of watermarks recommended.

A paper [8], proposed a method for using a phone equipped with a Smart Card Web Server (SCWS) SIM as a secure voter interface for e-voting, using the Prˆet `a Voter scheme as an example. The strengths of the proposed design are that it uses standardised protocols, hardware and communications to simplify its design and operation. The security of the standardized elements of the design has been extensively investigated by the expert community. Using existing tamper-resistant hardware (the SIM) with standardised features (SCWS) along with the MNO's Full Administration Protocol (via HTTPs), means that sensitive information can be protected at all times. The voting application is only available to the voter via an HTTPs connection from the mobile phone handset, and only authorised parties can access the SCWS voting application via the MNO network. Distributing web server functionality to voters' SIMs means that there is no central web server to target, and so an attacker must compromise many phones to successfully affect the election result. The use of the SIM's tamper-resistant environment for the storage and processing of sensitive voter credentials also addresses the secure platform problem. The principle of using a ubiquitous device (the phone) with SCWS to provide a secure distributed architecture for remote e-voting has been established. The voter will have a flexible and convenient 'vote-anywhere' capability in their phone, whilst the e-voting system is protected by making the effort required to attack it prohibitively high.

III. Propose Work

In internet voting if voting and operating environment is under control of voter's then there will be more chance of attacks such as denial of service attack. So to overcome this or minimize such attacks we can use poll site voting system in which voting and operating environment is under control of election officers.

Our proposed system will be consist of four phases as

- Registration phase
- Authentication phase
- Voting phase
- Counting phase

A. Registration Phase

In this phase some months before the election, voters can register them for voting by verifying their identity and address proof to election officer at pre-election camp and can get username and password. Register voter can change their password for security purpose.

In this phase election officers prepare voters list of the eligible voters. The device used for this phase will be arranged and manage and control by the election officers.

This information will be stored in authentication server (AS).

B. Authentication Phase

When voter login at polling booth on voting day using username and password on authentication server (AS) for voting, a registered voter get an UID, with this a voter can only cast vote once.
Also an authentic voter gets ballet and public encryption keys E1, E2, En for voting and encryption.

C. Voting Phase

Voters votes and encrypt the ballet on authentication server (AS). Authentication server will perform digital signature on encrypted ballot by voter and delivered it Counting Server.
At the Counting server, it checks the authentication of received ballot by verifying digital signature on it. And it sends back acknowledgment to the authentication server. Authentication server gives confirmation to the voter about his/her voting.

C. Counting Phase

After receiving data from AS the Counting Server (CS) first check its digital signature i.e. authentication of source. Prepare the table as

UID	Encrypted Vote

Fig. 1: UID Table

Then, the MIX-NET operation will perform on previous table as shown in fig.

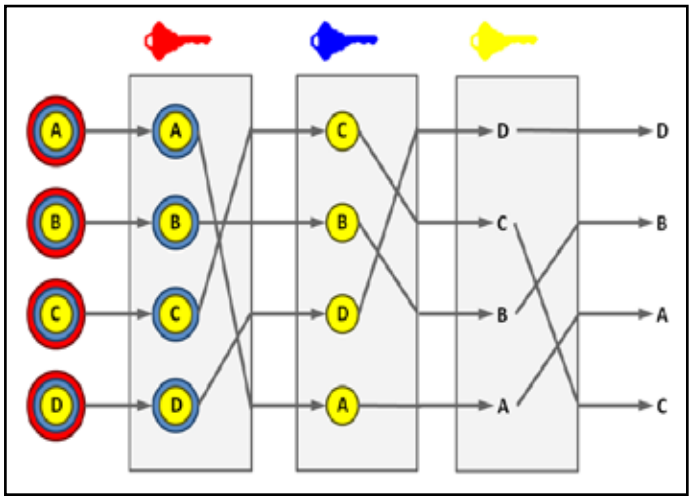

Fig. 2: Shafling Mixnet

At the time of result declaration decryption will be performed on encrypted votes by different private decryption keys.
Different authorities have control over different key, so to completely decrypt voter's vote to plain text a collective efforts of all the keys will required.
Plaintext votes will be counted and result will also be declared.

IV. Design of Software

The voter at client site communicates with Authentication server at server site. Similarly the authentication server communicates with the Counting server.
Since availability is key for the voting, every component of the system can be available by using the redundancy of the components.
Also security is also key issue in the internet voting system, cryptography and digital signature will be use for security purpose.
Since it is poll site Internet voting devices or systems use for the voting is installed and managed by the election officers.

V. Conclusion

In our proposed system, we are interested in poll site internet voting, for availability we will use redundancy of components of the system. For security and confidentiality we will be interested in digital signature and cryptography. Also we will provide security by using the concept of digital signature and encrypting ballot paper by more than one encryption key and also decrypting by more than one decryption key also we will use mixnet for conflict.

References

[1] Chun-Ta Li, Min-Shiang Hwang, Yan-Chi Lai,"A Verifiable Electronic Voting Scheme Over the Internet", 2009 Sixth International Conference on Information Technology: New Generations.
[2] Amir Omidi, Mohammad Abdollahi Azgomi,"An Architecture for E-Voting Systems Based on Dependable Web Services", 2009 IEEE.
[3] R.O. Ocaya,"A framework for collaborative remote experimentation for a physical laboratory using a low cost embedded web server", Journal of Network and Computer Applications, March 2011.
[4] Seo-Il Kang, 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
[5] Haijun Pan, Edwin Hou, Nirwan Ansari,"Ensuring Voters and Candidates' Confidentiality in E-voting Systems", 2011 IEEE.
[6] Amir Omidi, Saeed Moradi,"Modeling and Quantitative Evaluation of an Internet Voting System Based on Dependable WebServices", 2012 IEEE.
[7] Y ousfi Souheib, Derrode Stephane,"Watermarking in e-voting for large scale election", 2012 IEEE.
[8] Lazaros Kyrillidis, Sheila Cobourne, Keith Mayes, Song Dongy, Konstantinos Markantonakis,"Distributed e-Voting using the Smart Card Web Server", 2012IEEE.

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.