

A Survey on Online Voting System

Prof. Jagdish B. Chakole
Deptt. of Computer Technology
R.G.C.E.R., Nagpur, Maharashtra (India)
jagdishchakole@gmail.com

Prof. Samir Ajani
Deptt. of Computer Science & Engineering
R.C.O.E.M., Nagpur, Maharashtra (India)
ajanisn@rknec.edu

Abstract: - Nowadays there are so many online voting systems have proposed based on different techniques for security concern, this paper study review of some such systems.

In our proposed system, we are interested in secure online internet voting, which uses biometrics and cryptography approach for security concern.

Keywords: *Online internet voting, Voting client ,voting server, Encryption and Decryption.*

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:

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

- 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.
- 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 creation of a voting system by providing a cost effective solution to the government along with ensuring non-traceability and integrity of the votes cast while providing great convenience to voters. This system is developed robustly to ensure that all eligible voters having a Universal Identification Number of their country (For Example the Smart Card in USA) is allowed to cast their respective vote. The voters, who cast multiple votes during the process of voting is ensured to be prevented. Also to ensure the maintenance of authenticity, any biometric identification of the voters could be used for accessing the terminal to cast their vote and restricting them to cast again. The process of online voting could be deployed with three phases - the voter registration online vote capturing and the instant online counting and result declaration. A Secret Voting Password provided to voter during registration acts as an authentication mechanism which enables the voters to securely cast their vote along with their captured biometric identification. A Simulation result of implementation of the same is describing the robustness of this system.

A paper [2], proposed that an online voting system has become an interesting topic in recent years and most governments in Europe and elsewhere are taking steps to experiment as well as implement it to a great extent. Recent election problems in Bangladesh have sparked great interest in managing the election process through the use of internet. The present form of voting in general elections is founded upon entirely paper based and largely manual voting procedures. New technology for managing elections may entail several advantages. It may enhance the voters' scope for participating in the election as well as create scope for more rapid tallying of votes and distribution of seats. This enables the election commission to promptly announce the

election results within a short time. The risk of error in vote-tallying can also be largely eliminated and through all these steps, the elections can be made fair. In this paper we have proposed an online based voting system to eliminate the problems and bottlenecks of the traditional voting system in Bangladesh.

The proposed method in paper [3] describes an online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high security password is confirmed before the vote is accepted in the main database of Election Commission of India. The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party. In this model a person can also vote from outside of his/her allotted constituency or from his/her preferred location. In the proposed system the tallying of the votes will be done automatically, thus saving a huge time and enabling Election Commissioner of India to announce the result within a very short period

A paper [4] proposed a system Using Cryptography and Steganography at the same time, they try to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for Steganography and as keys for Cryptography. The key image is a Biometric measure, such as a fingerprint image. Proper use of Cryptography greatly reduces the risks in these systems as the hackers have to find both secret key and the template. The basic idea is to merge the secret key with the cover image on the basis of key image. The result of this process produces a stego image which looks quite similar to the cover image but not detectable by human eye. The system targets the authentication requirement of a voting system.

A paper [5], says that despite governmental efforts to facilitate elections and voting procedures for citizens in Jordan, there is a need for more governmental initiatives to ensure a high level of participation by voters in the election process, in particular, in the parliamentary election. The author introduces the concept of e-voting as one potential governmental initiative that would provide the citizenry with a new method of voting. Therefore, it is necessary to investigate people's interaction with e-voting and to address the main factors that may influence their intention to engage with e-voting as a new way of choosing their representative in parliament. This study used an established e-government adoption model to present the main predictors for voters' intentions to use an online voting system. By addressing these factors, the government in Jordan could build a strategy to market and introduce e-voting as a new method of choosing members of the House of Representative. This research paper provides a foundation for future empirical studies on e-voting adoption.

A paper [6], convey that with the increase in popularity of electronic voting, it has become necessary to have secure online voting mechanism. This paper presents a novel online voting scheme by using combination of biometric and password based security. The scheme uses Fuzzy Extractor to provide biometric based authentication, while secret password is used to provide password based protection of the voter. In addition, Pairing-Based Cryptography is used to provide the necessary security

requirements of an online voting system. A prototype of the proposed scheme is implemented and its performance and security analysis shows that the proposed scheme is cost-effective and at the same time satisfies the security requirements of an online voting system.

A paper [7], review Internet voting developments in Canada which is growing quickly, with activity focused in local elections, political party leadership votes and unions. In some instances, the federal structure of the Canadian state facilitates Internet voting use, while in others it inhibits it. The result of this system of divided jurisdiction is that Internet voting use in Canada resembles a patchwork, showing strong concentration in some areas and no penetration in other places. In addition to scattered geographic use, a variety of approaches to implementation are employed. In some cases online ballots are complementary to paper, while in others elections are now fully electronic. I-voting can be a two step process requiring registration or a more direct one-step voting procedure. Likewise, Internet voting is offered in the advance portion of certain elections, whereas in others it is available for the full voting period. Finally, given that private companies administer the Internet voting portion of elections there is also a mixture of technology.

III. PROPOSE WORK

Our proposed system consist of four phases as

- 1) Registration phase
- 2) Authentication phase
- 3) Voting phase
- 4) Counting phase

1) Registration phase:

In this phase registration is made manually by admin, who will check authentication of voter manually and give him/her unique id and password. Later on voter can change password.

2) Authentication phase:

When user login his account first time he has to input biometric. First level of authentication is done by voter biometric. Also voter also have a asymmetric key pair.

3) Voting phase:

Voting system has a asymmetric key pair.

At the time of voting voter login using biometric and while casting vote, first casted ballot will be encrypted using system public key. Another copy of that casted ballot is made on client system and copy of encrypted ballot is again encrypted by voter private key and generates two time encrypted copy and both copies are sending separately to voting server.

Voting server checks secrecy of casted ballot by decrypting two time encrypted ballot by voter public key and compare encrypted copy with one time encrypted copy, if both same then received data is secrete otherwise discarded and message is sent to voter

4) Counting phase:

At the time of counting all stored one time encrypted votes are decrypted by system private key. And that plaintext ballots are use for counting.

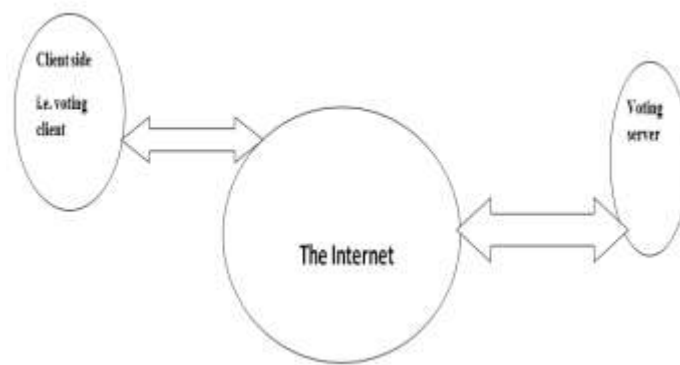


Figure 1: overview of proposed system

IV. CONCLUSION

In our proposed system, we are interested in Security of casted vote when it is travelling from voter to server. By this approach we can provide security from passive as well as active intruder.

REFERENCES

- [1] srivatsan sridharan “implementation of authenticated and secure online voting system”, july 2013 fourth international conference on computing, communications and networking technologies (icccnt)
- [2] Mohammad Shabbir Hasan; Abdullah Al Mahmood; Quazi Farhan, “A Roadmap Towards the Implementation of an Efficient Online Voting System in Bangladesh” 2010 International Conference on Computational Intelligence and Software Engineering (CiSE),
- [3] Himanshu Agarwal; G. N. Pandey,” Online voting system for India based on AADHAAR ID”, 2013 11th International Conference on ICT and Knowledge Engineering (ICT&KE), Pages: 1 - 4, DOI: 10.1109/ICTKE.2013.6756265.
- [4] Shivendra Katiyar; Kullai Reddy Meka; Ferdous A. Barbhuiya; Sukumar Nandi “Online Voting System Powered by Biometric Security Using Steganography”, IEEE 2011 International Conference on Emerging Applications of Information Technology (EAIT), DOI: 10.1109/EAIT.2011.70
- [5] Mohammad Kamel Alomari Towards E-democracy in the middle east: E-voting adoption DOI: 10.1109/ICITST.2014.7038780 ©2014 IEEE.
- [6] Nazatul Haque Sultan; Ferdous Ahmed Barbhuiya; Nityananda Sarma “PairVoting: A secure online voting scheme using Pairing-Based Cryptography and Fuzzy Extractor”, 2015 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), DOI: 10.1109/ANTS.2015.7413634
- [7] Nicole J. Goodman; Jon H. Pammett, “The patchwork of internet voting in Canada 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), DOI: 10.1109/EVOTE.2014.7001134 ©2014 IEEE