Indian Journal of Science and Technology

Supplementary Article

Highly Secured Online Voting System over Network

K. P. Kaliyamurthie[1*], R. Udayakumar[2], D. Parameswari[3] and S. N. Mugunthan[4]

[1]Professor & Head, Deptartment of IT, Bharath University, Chennai-600073, India; kaliyamurthie@bharathuniv.ac.in
[2]Professor, Department of IT, Bharath University, Chennai-600073, India; rsukumar2007@bharathuniv.ac.in
[3]Sr. Assistant Professor-MCA, Jerusalem College of Engineering, Chennai-600073, India; P_kaliyamurthie@gmail.com
[4]MCA, Jerusalem College of Engineering, Chennai-600073, India; snmugundan2013@gmail.com

Abstract

Internet voting systems have gained popularity and have been used for government elections and referendums in the United Kingdom, Estonia and Switzerland as well as municipal elections in Canada and party primary elections in the United States. Voting system can involve transmission of ballots and votes via private computer networks or the Internet. Electronic voting technology can speed the counting of ballots and can provide improved accessibility for disabled voters. The aim of this paper is to people who have citizenship of India and whose age is above 18 years and of any sex can give their vote through online without going to any physical polling station. Election Commission Officer (Election Commission Officer who will verify whether registered user and candidates are authentic or not) to participate in online voting. This online voting system is highly secured, and its design is very simple, ease of use and also reliable. The proposed software is developed and tested to work on Ethernet and allows online voting. It also creates and manages voting and an election detail as all the users must login by user name and password and click on his favorable candidates to register vote. This will increase the voting percentage in India. By applying high security it will reduce false votes.

Keywords: Internet Voting, e-voting, Face Recognition, Image Processing, Secured Network, JDBC.

1. Introduction

The present form of voting in general elections in India is founded entirely on paper based and largely manual voting procedures. New technology with advanced vote-client machines (computer terminals used for voting) for elections may entail several advantages. It may, enhance the voters' scope for participating in the election. It also creates scope for more rapid tallying of votes and distribution of seats. This also enables the electoral administration to promptly announce the election results to a broader circle. The risk of error in vote-tallying can also be largely eliminated.

The new technology also entails disadvantages that must be considered. One is the difficulty of guaranteeing ballot secrecy with absolute certainty. Another is the question of how to guarantee the reliability of the system, i.e. that the system will in all situations function in the manner in which it is meant to function. Another disadvantage is the expense of development and operation. All in all, then, the primary considerations are security and reliability.

In this proposed system, 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.

** Corresponding author:*
K. P. Kaliyamurthie (kaliyamurthie@bharathuniv.ac.in)

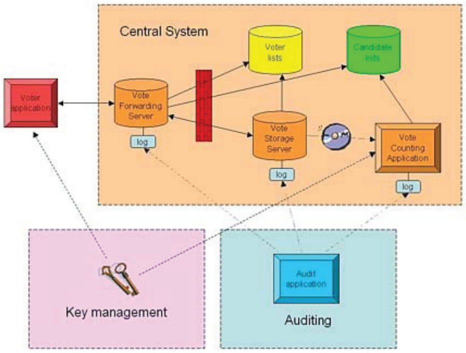


Figure 1. Architecture of online voting.

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. Figure 1 shows the architecture of the voting system through online.

2. Problem Background

This paper addresses the question of what Internet voting may mean. Our intent is not to propose a particular online voting solution, but rather to provide input to a future government committee or task force that may be created to delve further into the topic.

The potential benefits and risks of Internet voting are discussed in terms of seven of the core democratic principles that shape modern electoral systems: accessibility, equal voting power, secrecy, security, audit ability, transparency, and simplicity.

3. Problem Statement

Internet voting is about making the act of voting as convenient as possible and it holds great promise to improve accessibility, particularly to those who are absent from the jurisdiction, live in a remote area, or who have mobility issues. However, this voting channel introduces risks to some of the fundamental principles of democratic systems. As policy makers consider a place for Internet voting, it is important that a balance is struck between competing principles, all of which are critical to electoral integrity, so that public confidence in election outcomes is maintained.

4. Research Objective

The main objective of this work is to develop an interactive voting system application with which users can participate using their information stored prior in database while creating the voter ID and the information need to be updated at an period of less than six months for perfect user verification by the Independent Electoral Commission of India (IECI). In this system people who have citizenship of India and whose age is above 18 years and of any sex can give their vote through online without going to any physical polling station.

After registration each voter/user is assigned with the particular ID generated by the Electoral Commission of India along with the online registration ID i.e. user name. With every time logging into the system the user is validated with both of the ID. Through these development we can obtain a secured website comprises of all the voting methodologies in a single website.

5. Scope of Study

The scope of the work is that it will use the ID and password created by user to register him/her in the voting site, through this all the details of voter are saved in database. And it will act as the main security to the votes system.

Advanced technology: It is an advanced technology used now a day. It increases the internet knowledge of the users which is very necessary for current generation.

Internet: It is an online facility and hence very useful for the users. Voters can vote from anywhere at any time in India.

E-Mails: Election Commission can send the error report to a particular user if he/she entered false information.

Image: Image is being captured through online and that image is being validated with the image on the database.

Traditionally in a manual, paper based election system, voters have to reach at polling stations to cast their votes by standing in a long queue, therefore it is very much difficult for voters to vote their votes in this way there is a low rate of vote casting [1]. In 2004, Chaum [Ch04] and, independently, Neff [Ne04] proposed 316 cryptographically secure voting systems in which the voter has access to no computational device at the time of voting. Since then, most research has focused on such bare-handed, end-to-end verifiable voting systems [2].

In 2004, the Department of Defense cancelled the Internet-based voting system SERVE that was developed by Accenture on a $22 million contract [3, 4] because of justified security concerns raised by the academic community [5]. At the same time, the source code of currently used electronic voting systems was put under scrutiny and a multitude of flaws was unearthed [6].

In 2010, Washington, D.C. developed an Internet voting pilot project that was intended to allow overseas absentee voters to cast their ballots using a website [8]. Prior to deploying the system in the general election, the District held a unique public trial: a mock election during which anyone was invited to test the system or attempt to compromise its security [9]. There are some drawbacks with this system are, there can be software failure issue, insecure access of internet and also voter should be familiar with internet [7].

In our proposed system we proposed new Blind signature which is a special form of digital signature, which was introduced by David Chaum in 1982 [13], in which the content of a message is blinded before signature. In blind signature scheme, signer signs on the blind message using his/her private key and anyone can verify the legitimacy of the signature using signer's public key [14].

This software is being developed for use of e-voting. Here each user is registered with the application. After registration each voter/user is assigned with the particular ID generated by the Electoral Commission of India along with the online registration ID i.e. user name. With every time logging in to the system the user is validated with both of the ID. Through these development we can obtain a secured website comprises of all the voting methodologies in a single website.

Internet voting presents a challenge to policy makers. On the positive side, Internet voting fits with the B.C. government policy direction to provide citizens with access to a greater variety of high quality online services [11, 12]. Internet voting offers voters a convenient alternative to in-person voting. This may be particularly important to voters who have difficulty attending in-person voting opportunities. And finally, concerns about the digital divide are diminishing as the proportion of British Columbians who use the Internet continues to grow [15, 16].

Policy makers need to weigh these positive considerations with compromises that Internet voting would entail for several foundational principles of elections. With the current state of technology, Internet voting is considered to be less effective than traditional, in-person and postal voting methods at protecting ballots against larges cale fraud, ensuring the secrecy of the vote, and providing a fully transparent and observable process that can be effectively audited. Because specialized computer skills are required to observe an Internet voting process, voters would have to delegate their trust to "experts" to confirm that the election is conducted properly [18, 19].

Through these methodologies an objective of this research is to capture the image through camera at the time of logging on to the page and it validates the image along with the password generated. Then the particular login is authenticated.

6. Design and Implementation

Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems [17], or DRE). To increase the security of this e-voting system to another level which is quiet concern at different origins we have implemented an online image verification system.

The aim of this design is to develop an interactive voting system with which users can participate using their images stored prior in database [10] while creating the voter ID and the image need to be updated at an period of less than six months for perfect user verification. The project will involve three phases: the development of a graphical front-end to the voting system; the development of a method of interaction with *web cams*, and the development of a web-based administration tool. The new user must produce their photo while registering in the e-voting system.This should not be surprising. Almost weekly we learn of one system or another that is penetrated by outsiders, including teens and overseas criminals [20, 21].

Organizations that have been unable to protect networks and applications include banks, government agencies, the Department of Defense and ironically, Internet security firms. To the public, like some legislators, it seems intuitive to accept that "We use ATMs and bank online with no problems, why not vote that way?" This argument fails theoretically and practically. The anonymous ballot does not provide the verification and proof of banking receipts or double entry bookkeeping which help detect fraud [22, 23].

ATMs are bank-owned computers with special network security, much safer than general purpose computers [24]. Even so, banks lose billions each year to fraud with ATMs and online banking. The system is highly insecure and prone to election malpractice. Due to the fact that any student can come and fill out a ballot sheet without prior authentication to determine who he/she says they are, is a major concern [25, 26].

7. Algorithm

Recent work on face identification using continuous density Hidden Markov Models (HMMs) has shown that stochastic modelling can be used successfully to encode feature information. When frontal images of faces are sampled using top-bottom scanning, there is a natural order in which the features appear and this can be conveniently be modelled using a top-bottom HMM. However, a top-bottom HMM is characterised by different parameters, the choice of which has so far been based on subjective intuition. This paper presents a set of experimental results in which various HMM parameterisations are analysed. Matlab is used to implement the Eigenfaces, Fisherfaces, and SIFT matching algorithms. The following algorithm states the work of Principal Component Analysis (PCA):

Principal Component Analysis:

```
p = a random vector
do $c$ times:
t = 0 (a vector of length $m$)
for each row $x \in X^T$
$t = t + (x \cdot p)\, x$
$p = \frac{t}{|t|}$
return p
```

8. Methodology

Every voter should have a personal identification number. This number will be automatically checked along with the ID stored on the database. Let us use 256*256 pixels bitmap cover image which should be clear so that it will be very easy for comparison. This image will be chosen from among a set of images in the system which matches the cover image. Cover image is a simple image for personal identification over the base image. So, the cover image for each voter is different which will reduce the chances of predicting the image by an attacker during transmission.

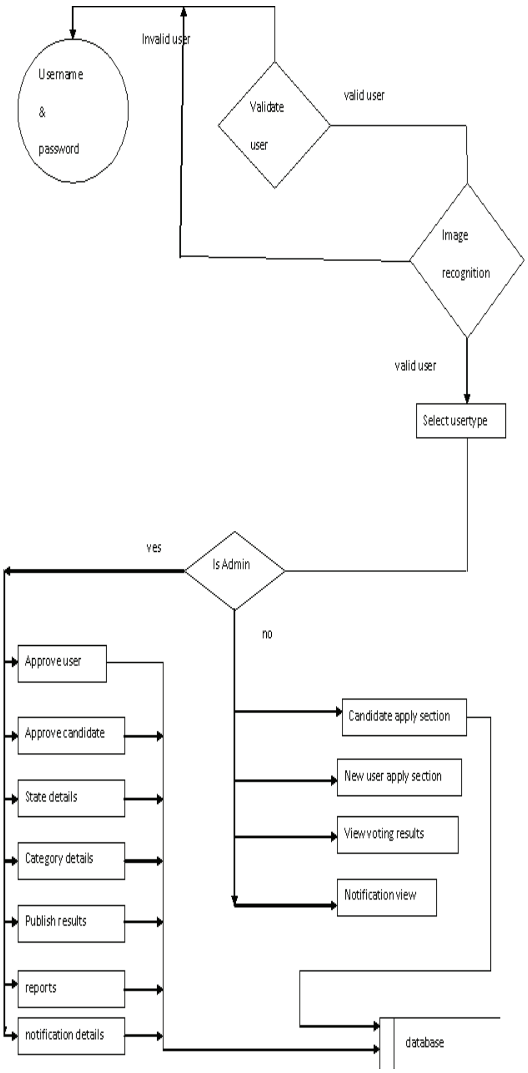


Figure 2. Work flow.

9. Workflow

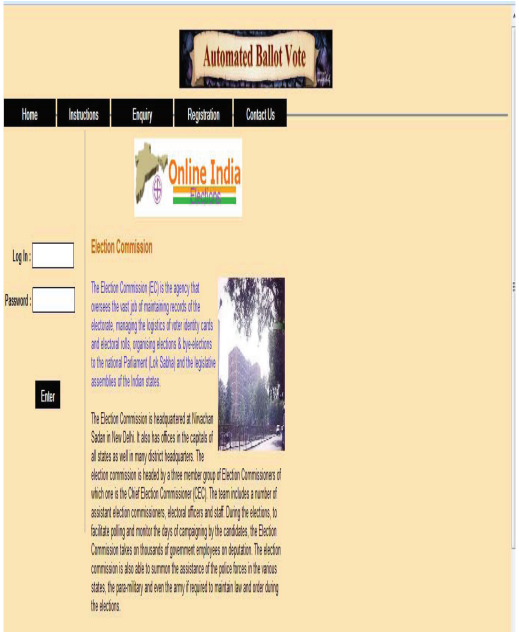
The Figure 2 shows the workflow where the user identity and a perfect image is being compared and validated.

10. Experimental Result

Voting System needs the verification of the user through the username and password and the Figure 3 shows the home page along with the login panel.

From the above page while login the image stored on the database is compared with the image taken while authentication is done through Figure 4.

After perfect authentication is made then the user can vote up for the desired candidate as the Figure 5.



Election Commission

The Election Commission (EC) is the agency that oversees the vast job of maintaining records of the electorate, managing the logistics of voter identity cards and electoral rolls, organising elections & bye-elections to the national Parliament (Lok Sabha) and the legislative assemblies of the Indian states.

The Election Commission is headquartered at Nirvachan Sadan in New Delhi. It also has offices in the capitals of all states as well in many district headquarters. The election commission is headed by a three member group of Election Commissioners of which one is the Chief Election Commissioner (CEC). The team includes a number of assistant election commissioners, electoral officers and staff. During the elections, to facilitate polling and monitor the days of campaigning by the candidates, the Election Commission takes on thousands of government employees on deputation. The election commission is also able to summon the assistance of the police forces in the various states, the para-military and even the army if required to maintain law and order during the elections.

Figure 3. Home page.

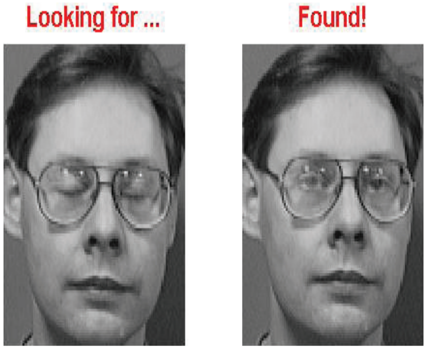
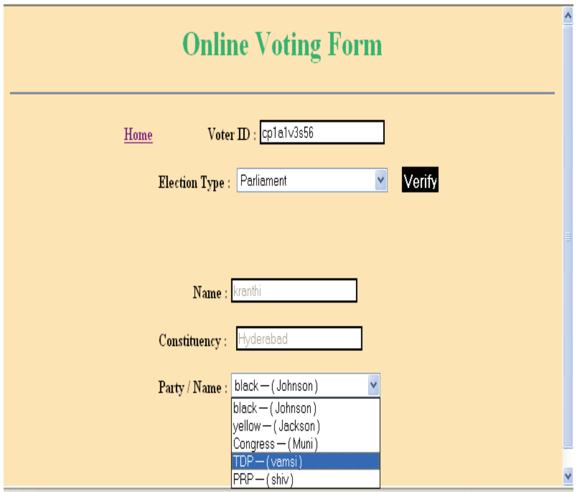


Figure 4. Image recognition.



Voter ID : cp1a1v3s56

Election Type : Parliament

Name : kranthi

Constituency : Hyderabad

Party / Name : black – (Johnson)

black – (Johnson)
yellow – (Jackson)
Congress – (Muni)
TDP – (vamsi)
PRP – (shiv)

Figure 5. Voting page.

11. Conclusion

In this paper we have enforced a method for integrating Cryptography over network to present a highly secure Online Voting System. The security level of our system is greatly improved by the new idea of random cover image generation for each voter. The user authentication process of the system is improved by adding both face recognition and password security. The recognition portion of the system is secured by the cover image. This system will preclude the illegal practices like rigging. Thus, the citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy. The usage of online voting has the capability to reduce or remove unwanted human errors. In addition to its reliability, online voting can handle multiple modalities, and provide better scalability for large elections. Online voting is also an excellent mechanism that does not require geographical proximity of the voters. For example, soldiers abroad can participate in elections by voting online. Hence, by this voting percentage will increase drastically.

12. References

1. Mercuri R (2000). Electronic vote tabulation checks and balances, Ph.D. Thesis, University of Pennsylvania, Philadelphia, PA.
2. Ben-Nun J, Farhi N et al. A new implementation of a dual (Paper and Cryptographic) voting system.
3. Swaminathan B, and Dinesh J C D (2012). Highly secure online voting system with multi security using biometric and steganography, International Journal of Advanced Scientific Research and Technology, vol 2(2), 195–203.
4. Schwartz J (2004). Online voting canceled for Americans overseas, The New York Times.
5. Jefferson D, Rubin A et al. (2004). A security analysis of the secure electronic registration and voting experiment (SERVE), Technical report, Available From: http://servesecurityreport.org.
6. Kohno T, Stubblefield A et al. (2004). Analysis of an electronic voting system, IEEE Symposium on Security and Privacy, 27–40.
7. Anand A, and Divya P (2012). An efficient online voting system, International Journal of Modern Engineering Research, vol 2(4), 2631–2634.
8. Kellerher W J. The Internet Voting Research and Education Fund Twitter: wjkno1, Available From: http://ssrn.com/abstract=2229557.
9. Wolchok S, Wustrow E et al. (2012). Attacking the Washington, D.C. Internet voting system, vol 7397, 114–128.

10. Available From: http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html
11. Adida B (2008). Helios: web-based open-audit voting, Proceedings of the 17th USENIX Security Symposium, 335–348.
12. Rubin A (2006). Security considerations for remote electronic voting over the Internet, vol 55(4), 193–202. Available From: http://avirubin.com/e-voting.security.html
13. Chaum D (1988). Blind signature systems, U.S. Patent 4, 759, 063.
14. Tan Z, Liu Z et al. (2002). Digital proxy blind signature schemes based on DLP AND ECDLP, MM Research Preprints, 212–217.
15. ECDLP MM Research Preprints, 212–217.
16. Daily Times, PPP wants fresh election in Bannu, Available From: http://www.dailytimes.com.pk/default.asp?page=2007%5C04%5C03%5Cstory_3-4-2007_pg11_2
17. Monitory Report (2002). Available From: http://action.web.ca/home/sap/attach/pk%20election %20monitor%202002.rtf
18. Gilberg J (2003). E-Vote: an Internet-based electronic voting system: consolidated prototype 2 documentation, Technical Report e-VOTE/WP-7/D7.4/3.0/29-05-2003, Available from: http://www.instore.gr/evote/evote end/htm /3public/doc3/public/public deliverables/d7 4/ Consolidated Docu final.zip.
19. Damgård I, Groth et al. (2003) Secure electronic voting, Chapter 6, Kluwer Academic Publishers, 77–99.
20. Riera A, and Brown P (2004). Bringing confidence to electronic voting, EJEG, vol 2(1).
21. Lin Y, and Chlamtac I (2000). Wireless and mobile network architectures, Wiley Publications 0–99.
22. Baron R J (1981). Mechanisms of human facial recognition, International Journal of Man-Machine Studies, vol 15, 137–178.
23. Cardinaux F, Sanderson C et al. (2006). User authentication via adapted statistical models of face images, IEEE Transactions on Signal Processing, vol 54(1), 361–373.
24. Lee K-C, Ho J et al. (2005). Acquiring linear subspaces for face recognition under variable lighting, IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), vol 27(5), 684–698.
25. Maturana, D, Mery D et al. (2009). Face recognition with local binary patterns, spatial pyramid histograms and naive bayes nearest neighbor classification, 2009 International Conference of the Chilean Computer Science Society (SCCC), 125–132.
26. Rowley H, Baluja S et al. (1998). Neural network-based face detection, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol 1(20), 23–28.