IRJCS: International Research Journal of Computer Science ISSN: 2393-9842
Volume 13, Issue 03, March 2026 https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.30

Online Voting System

Dr.M.Sakthivel
Head, Department of Computer Science and Engineering
Sengunthar Engineering College (Autonomous), Tiruchengode, India
csehod@scteng.co.in
https://orcid.org/0000-0003-4163-6630
Rajan Kumar Varnwal,Sani Kumar Gupta,Om Kumar
Department of Computer Science and Engineering
Sengunthar Engineering College (Autonomous), Tiruchengode, India
rajankumarvarnwal1234@gmail.com, sanikumargupta592@gmail.com
omkumarom527@gmail.com

Publication History
Manuscript Reference: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10109
Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10109
Received: 30, January 2026, Revised: 13, February 2026, Accepted: 28 February 2026 Published Online: 25 March 2026
https://www.irjcs.com/volumes/Vol13/iss-03/30.CSMR26.MRCS10109.pdf
Article Citation: Prof.Perumala,Rajan,Sani,Om(2026),Online Voting System,IRJCS: International Research Journal of Computer Science, Volume 13,Issue 03 of 2026 pages 273-278 **Doi:>** https://doi.org/10.26562/irjcs.2026.v1303.30
BibTeX Key Prof.Perumala@2026Online Orcid: https://orcid.org/0009-0004-9398-7488
IRJCS papers should be cited as IRJCS (International Research Journal of Computer Science, AM Publications, India 2026, ISSN 2393-9842, https://doi.org/10.26562/ijrcs.2025.v1303.30 The journal's official abbreviation is IRJCS.

Abstract: In the digital age, the demand for secure, efficient, and transparent voting mechanisms has become increasingly vital. The traditional paper-based voting systems, while reliable to some extent, are often time-consuming, resource-intensive, and susceptible to human error and electoral fraud. To address these challenges, this project presents the design and development of a comprehensive online voting system that aims to modernize the electoral process through the use of secure web technologies. The proposed system offers a convenient, user- friendly, and transparent method for eligible voters to cast their votes electronically from any location with internet access, thereby enhancing participation and reducing logistical barriers. The online voting system is developed to ensure core democratic principles such as security, integrity, confidentiality, transparency, accessibility, and verifiability. It incorporates advanced authentication mechanisms to verify the identity of voters, ensuring that only authorized individuals are allowed to vote. Techniques such as two factor authentication (2fa), biometric verification, or one-time password (otp) via email or SMS are integrated into the system to prevent impersonation and unauthorized access. To maintain the integrity and confidentiality of the voting process, the system uses end-to-end encryption and secure sockets layer (ssl) protocols. This ensures that the votes cast cannot be intercepted, altered, or traced back to the voter, preserving voter anonymity
Keywords: Online Voting System, E-Voting System, Secure Authentication, Database, Web Application, and Electronic Ballot.

I. INTRODUCTION

In many parts of the world, the advancement of technology has changed the way we vote, as electronic voting has been deployed in many different types of elections for several decades (Gibson, Krimmer, Teague, & Pomares, 2016). E- voting, also known as electronic voting, is a term that incorporates several types of voting, including both electronic means of casting a vote and electronic means of counting votes, such as punched cards, optical scan voting systems, and specialized voting kiosks (Elewa, Sammak, Abd El Rahman, & ElShishtawy, 2015). This method is perceived to reduce errors and improve the election process so that it becomes more accurate and ensures the integrity of the entire election procedure. One of the main issues with the existing manual voting system, such as paper-based voting, is that it is time-consuming and requires a considerable amount of time to cast and count votes. In addition, it can also produce fake or unreliable results. Therefore, this traditional method needs to be upgraded, and there is a growing need to shift from the manual voting system to a more sophisticated and digitalized voting platform. Fake voting is also related to the issue of intelligibility. As mentioned by Munisami (2018), a paper- based polling system that uses pens, stamps, punch cards, or ballots can produce ambiguous results. He further explained that the possibility of result manipulation by influencing authorities could occur if the manual voting process is not properly conducted. Electronic voting (e-voting) is generally viewed as a supportive tool for making the election process more efficient and effective. If e-voting is properly implemented and managed, it can ensure the safety of ballots, speed up the processing of results, and make the overall voting process easier for voters. This paper aims to present users' perspectives one-voting the researchers), which include their experience of the voting process, satisfaction levels, and interaction with the system, as well as to identify the usability criteria of thee-voting interface as an enhancement. The findings of the study will provide valuable insights to guide decision-makers in customizing the proposed system to meet specific voting needs, particularly for adoption within university environments or other community-based organizations. Furthermore, e-voting can help increase voter participation, reduce election costs, and improve the accuracy and reliability of election results. Cryptography generates a ciphertext, while steganography produces a stage-object which is not perceptible by Human Visual System (HVS).

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.30

In electronic voting, cryptography is a commonly used technique as it is a good defence against threats. In this paper, the authors introduce a novel approach to enhance E2E Voting System's security by combining visual cryptography with image steganography. Image steganography is chosen due to its capability to use data transmitted over the network. During the election voting process, the image steganography protects the existence of the message as a secret (Wang and Wang, 2004), offering a good solution for threats and risks that might occur. The combination of these two schemes is expected to produce an improved and secure approach (Morkel et al., 2005). Petcu & Stoichescu (2015) proposed a mobile biometric-based design that uses techniques such as Secure Sockets Layer encryption, certificate keys and security tokens. This paper is organized as follows.

LITERATURE REVIEW

The evolution of technology and the widespread use of the internet have transformed many aspects of human life, including communication, commerce, and governance. One of the most significant innovations in the field of governance is the development of online voting systems (e- voting). Online voting systems are designed to allow eligible voters to cast their votes electronically, using computers or mobile devices connected to the internet, rather than traditional paper-based ballots. This system aims to increase voter participation, reduce election costs, and enhance transparency and efficiency in the electoral process. Several studies and research efforts have explored the design, security, and usability of online voting systems. According to Rivest and Wack (2006), the main goal of e- voting is to provide a secure, reliable, and verifiable voting process that ensures confidentiality, integrity, and authenticity. Security remains one of the most critical concerns in e-voting. Researchers emphasize the need for mechanisms that prevent vote tampering, ensure voter anonymity, and provide verifiable audit trails. Technologies such as block chain, cryptographic encryption, and biometric authentication have been proposed to enhance system security and build public trust. Nye and Adams (2017) highlighted that online voting systems must be user-friendly to encourage adoption among all age groups, including those with limited technical skills. Usability studies reveal that a well-designed user interface, clear instructions, and accessibility features significantly improve voter confidence and satisfaction. Moreover, systems must be adaptable to multiple platforms desktop, mobile, and tablet to ensure universal accessibility. In recent years, blockchain-based voting systems have attracted significant attention. Zheng et al. (2019) proposed that blockchain provides a decentralized and tamper-proof ledger that records vote securely and transparently. Each vote is stored as a transaction in the blockchain, ensuring immutability and verifiability. This approach addresses many traditional voting challenges such as vote duplication, ballot manipulation, and unauthorized access. However, scalability and privacy issues remain key challenges in block chain implementation for national elections.

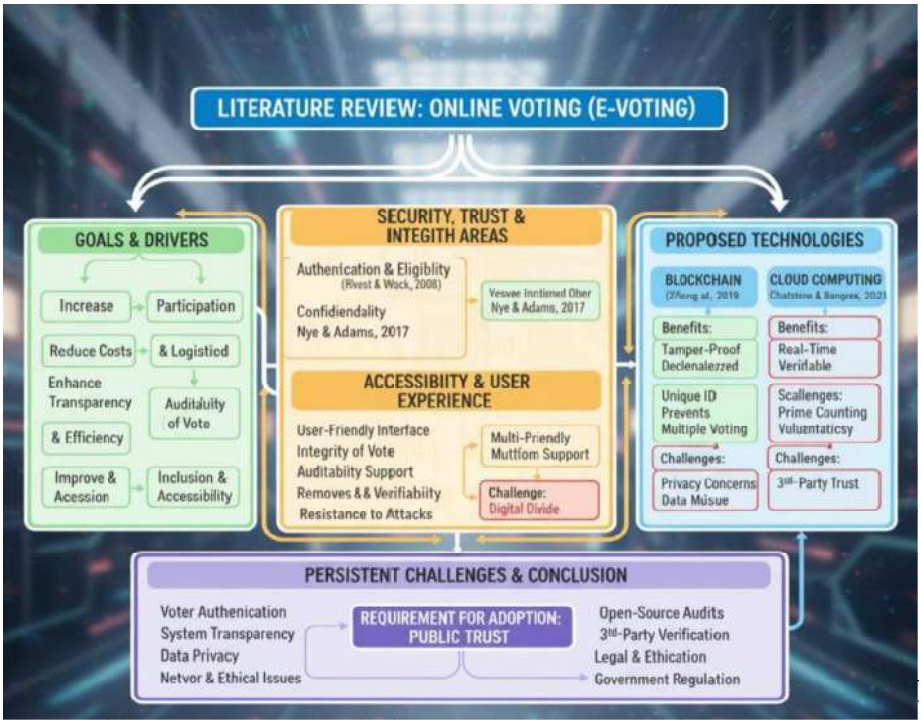

Fig.1: Flowchart of E-Voting Literature Review

Another major contribution to e-voting research focuses on biometric authentication systems. According to Adebayo et al. (2020), integrating fingerprint or facial recognition ensures that each voter is uniquely identified and eliminates multiple voting attempts. However, privacy concerns arise due to the storage and misuse of biometric data, requiring strict data protection policies and encryption standards. Cloud computing has also played an important role in recent online voting developments. It enables scalable storage, real-time vote counting, and system redundancy. Researchers such as Chatterjee and Banerjee (2021) suggest that cloud-based architectures reduce costs and improve reliability, especially in large- scale elections. However, reliance on third-party cloud providers introduces potential vulnerabilities if not properly secured.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.30

The integration of cloud computing into voting systems has enabled scalable and reliable election infrastructures. Cloud-based systems allow for Realtime data processing, secure data storage, and efficient system redundancy. According to Chatterjee and Banerjee (2021), cloud platforms support large scale elections by handling thousands of simultaneous voter requests while maintaining uptime and reliability. Security, Trust and Integrity: One of the most widely researched topics is the security of online voting systems. The literature divides major concerns into several categories: Authentication & eligibility: Ensuring only eligible voters cast tokens, and each votes once.

Methods include digital IDs, biometrics, multi- factor authentication, and OTPs.

a) Confidentiality & anonymity: The system must protect voter privacy while assuring that votes are linked to legitimate voters (yet cannot be traced back to disrupt secrecy).
b) Integrity of vote transmission and storage: Votes must travel securely from the voter's device, be stored without tampering, and be counted correctly. Encryption, secure channels (TLS), end-to-end verifiability are discussed.
c) Auditability and verifiability: Many authors emphasize that a major strength is systems where voters and independent auditors can verify that votes were cast and counted correctly without exposing voter identity. Some systems propose voter-receipts or cryptographic proofs.
d) Resistance to attacks: The literature points out multiple threats malware on voter devices, denial- of-service attacks on voting servers, insider fraud, coercion, vote-selling, and nation-state cyber- attacks.

SYSTEM IMPLEMENTATION

The implementation phase of the Online Voting System involves translating the system design and specificationsintoaworkingapplicationthroughastructureddevelopment process. This phase includes setting up the development environment, coding the front- end and back-end components, integrating databases, ensuring security mechanisms, testing, and finally deploying the system for actual use. The goal is to deliver a fully functional, secure, and user-friendly voting platform that meets the requirements defined during the system analysis and design stages.

1. Source Code: The implementation of the Online Voting System uses a combination of modern web development technologies:

a) Frontend: HTML5, CSS, JavaScript, Bootstrap, Node JS and optionally a framework. JS for a dynamic, responsive interface.
b) Backend: PHP, or Node.js to handle server-side logic. Database: MySQL, or MongoDB for storing user data, votes, and election results securely.
c) Authentication & Security: JWT (JSON Web Tokens), SSL encryption, and Dummy OTP-based verification to ensure secure login and voting.
d) Deployment: Hosted on cloud platforms such as AWS, Heroku, or Digital Ocean with server configurations managed using NGINX or Apache.

2. System Testing: System testing is a critical phase in the implementation process that validates the functionality, performance, security, and reliability of the Online Voting System before deployment.

Functional Testing:

a) User Registration and Login: Verified that users can register, receive activation emails/OTPs, and log in successfully.
b) Vote Casting: Tested the voting process to ensure voters can view candidates, submit a vote only once, and receive confirmation.
c) Admin Controls: Confirmed admins can add/remove candidates, approve voters, and generate election results.
d) Result Generation: Ensured vote counting is accurate and results are displayed correctly.

Security Testing:

a) Authentication: Tested multiple login attempts, password recovery, and two-factor authentication robustness.
b) Data Encryption: Verified that votes are encrypted in transit and at rest.
c) Penetration Testing: Conducted simulated attacks such as SQL injection, cross-site scripting (XSS), and session hijacking to identify vulnerabilities.
d) Access Control: Checked role-based permissions ensuring voters and admins can only access authorized functions. Performance Testing.
e) Load Testing: Simulated hundreds to thousands of concurrent users to ensure the system remains responsive without crashes or significant delays.
f) Response Time: Measured time taken to submit votes and generate results, ensuring votes are processed within acceptable limits (less than 2 seconds).

SYSTEM DIAGRAM

The Online Voting application will help to manage the shop, customers, products, and bookings. It allows the shop owner to manage the day-to-day process of a Farming shop conveniently. We Have compiled structural UML diagrams i.e. component diagrams, and three types of behavioral UML diagrams i.e. Activity, Sequence, Component, and Use Case diagrams for the Online Voting Project. An online voting system project is designed to automate the voting system. where users can vote for a particular party from a list of multiple parties that can be involved in the election. The complete voting management project including admin and user side is available with source code, project report, and configuration on your machine.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.30

Fig.2: Architecture Diagram

CLASS DIAGRAM:

The Online Voting System class diagram represents the structure of the system through five main classes: Voter, Admin, Candidate, Vote, and Voting System. The Voter class stores details such as voter ID, name, email, password, and voting status. It allows users to register, log in, cast a vote, and view election results. The admin class manages the entire system by handling candidate information, viewing results, and maintaining data security. It includes attributes like admin ID, username, and password, with operations such as login, add candidate, remove candidate, and view results.

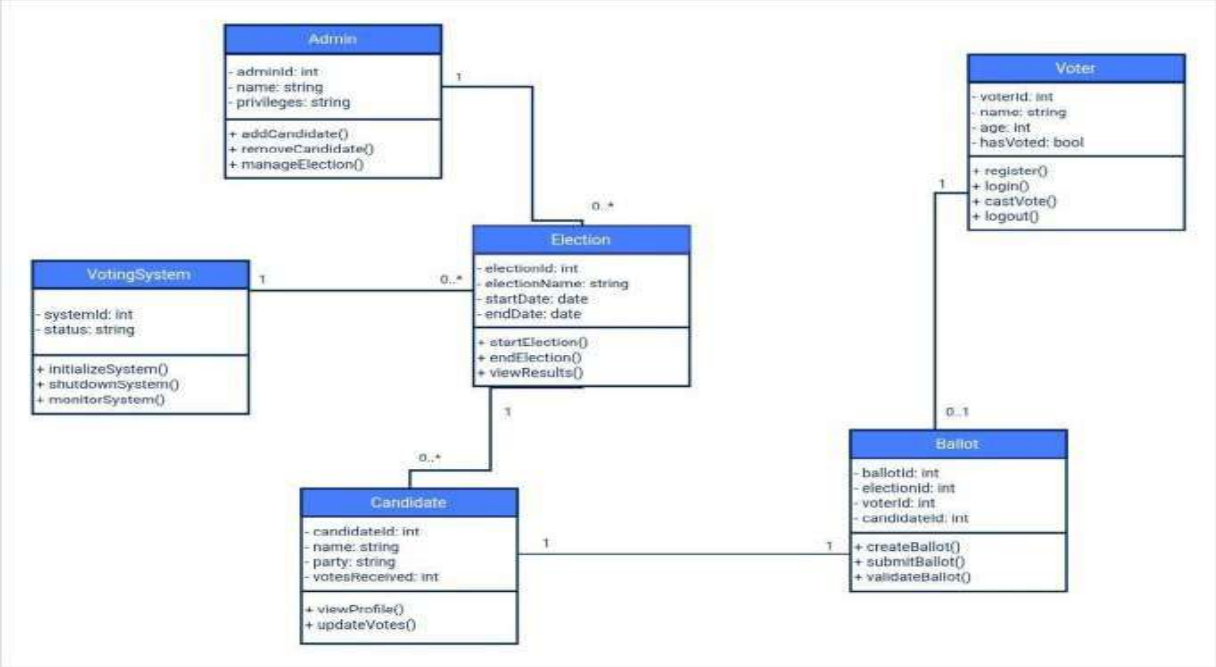

Fig .3: Class Diagram

PROPOSEDSYSTEM

The Online Voting System is designed as a digital alternative to the traditional voting method. It leverages modern web technologies and cyber security protocols to allow eligible voters to cast their votes remotely over the internet, using any digital device such as a computer, smart phone, or tablet. The system is built with several key modules, including user registration, voter authentication, candidate listing, vote submission, result calculation, and admin control panel. Voter authentication methods may include OTP verification, biometric scans, or integration with government-issued digital identity systems to ensure that only eligible voters can access the system and vote once.

A. User Authentication and Registration

Before the election period, voters are required to register through a secure portal. The system verifies their eligibility using a government-issued identification number, voter ID, or biometric data such as fingerprints or facial recognition.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.30

Once verified, each voter receives a unique digital credential or login key, which they can use to access the voting system during the election.

B. Vote Casting Module

Once authenticated, voters are presented with an electronic ballot that mirrors the traditional voting format. Candidates and parties are displayed clearly, and voters can make their selections by clicking their preferred option. The interface is designed to be intuitive and accessible, supporting multiple languages and assistive technologies for voters with disabilities.

C. Vote Encryption and Secure Storage

Security is a central feature of the proposed system. Advanced cryptographic algorithms, such as RSA or AES, are used to encrypt each vote. The system also employs block chain or distributed ledger technology to record transactions in a tamper-proof 18 manner. Each vote becomes a unique block linked to a chain, ensuring immutability and transparency.

D. Vote Counting and Verification

After the voting period ends, the system automatically decrypts and counts votes using a secure key controlled by an independent electoral authority. Since the votes are stored in encrypted form during transmission and storage, decryption can only occur at the counting stage.

E. System Analysis

System analysis is a crucial stage in the development of an Online Voting System (OVS). It involves understanding the system's objectives, identifying user requirements, analyzing existing systems (if any), and determining the most effective ways to design a secure, efficient, and user- friendly voting platform. The goal of this analysis is to ensure the proposed system fulfills all functional and non- functional needs while maintaining security and transparency in the election process.

CONCLUSION

The implementation of an Online Voting System represents a significant advancement in the modernization of democratic processes. As societies become increasingly digital, there is a growing need to leverage technology to make voting more accessible, efficient, and secure. This project has explored the key features, benefits, challenges, and potential impact of transitioning from traditional paper-based voting to a digital platform. One of the primary benefits of an online voting system is the convenience it offers to voters. By allowing individuals to cast their votes from any location with internet access, it increases voter turnout, especially among those who may be unable to visit polling stations due to physical disabilities, travel constraints, or demanding work schedules. Furthermore, it can reduce long queues at polling booths, minimize human errors, and streamline the entire election process. From an administrative perspective, online voting systems can significantly lower the cost and logistical complexities involved in organizing elections. Traditional methods require printing ballots, hiring personnel, and setting up polling stations costs that can be drastically reduced with a secure and well- designed digital system. Additionally, the speed of vote counting and result tabulation can be greatly improved, allowing for faster and more accurate election outcomes. The advent of digital technology has revolutionized nearly every aspect of human life, from communication and commerce to education and governance. One of the most significant applications of this technological advancement is the concept of online voting systems. Online voting (or e voting) represents a major step toward modernizing electoral processes, offering the potential to make elections more efficient, transparent, and accessible. After an in-depth exploration of the design, implementation, benefits, and challenges of an online voting system, it becomes clear 14 that while the technology holds immense promise, its successful adoption requires careful consideration of technical, legal, and social factors. At its core, the online voting system aims to simplify and secure the process of casting and counting votes through the use of web-based technologies. It eliminates many of the logistical barriers associated with traditional paper-based voting, such as the need for physical polling stations, manual vote counting, and extensive manpower. Through such mechanisms, an online voting system can maintain the confidentiality, integrity, and accuracy of election data.

REFERENCES

1. Chaum,D.(2001).SureVote:TechnicalOverview. Vote Here, Inc. Cranor, L.F.(1996). Electronic Voting. Communications of the ACM, 38(11), 88–89.
2. Fujioka,A.,Okamoto,T.,&Ohta,K.(1992).A Practical Secret Voting Scheme for Large Scale Elections. Advances in Cryptology AUSCRYPT '92, Springer.
3. Rubin, A.D.(2002).Security Considerations for Remote Electronic Voting over the Internet. Communications of the ACM, 45(12), 39–44.
4. Cetinkaya,O.,& Cetinkaya,D. 2007). A Secure Online Voting System Using Homomorphic Encryption. Proceedings of the 2007 International Symposium on Computer Networks.
5. Adams, A., & Laurie, B. (1999). Security of Electronic Voting Systems. Software Engineering Notes, 34(1), 18–26.
6. Alvarez, R. M., & Hall, T. E. (2003). Electronic Elections: The Perils and Promises of Digital Democracy. Princeton University Press.
7. National Science Foundation (NSF) Report (2001). Developing Trustworthy Elections. Washington, D.C.
8. Saltman, R. G. (2006). The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence. Palgrave Macmillan.
9. Cranor, L. F., & Cyton, R. K. (1997). Design and Implementation ofa Secure Online Voting System. IEEE Symposium on Security and Privacy.
10. Mercuri, R. (2001). Electronic Vote Tabulation: Checks and Balances. IEEE Computer, 34(3), 51– 57.
11. Rivest, R. L., & Wack, J. P. (2006). On the Notion of "Software Independence" in Voting Systems. NIST Information Technology Laboratory.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.30

12. Chaum,D.,Ryan,P.Y.A.,&Schneider,S.(2005). A Practical Voter-Verifiable 43 Election Scheme. Proceedings of the 10th European Symposium on Research in Computer Security (ESORICS 2005), Springer.
13. Fujioka, A., Okamoto, T., & Ohta, K. (1992). A Practical Secret Voting Scheme for Large Scale Elections.AdvancesinCryptology—AUSCRYPT '92, Springer.
14. Rivest, R. L. (2001). Electronic Voting: An Overview. Proceedings of the 2nd International Conference on Cryptology in India (INDOCRYPT 2001), Springer.
15. Rubin, A.D.(2003). Security Considerations for Remote Electronic Voting Over the Internet. Communications of the ACM, 45(12), 39–44.
16. Moyle, M.,& Goodman, S. E. (2002). The Case of Estonia: E-Government and E-Voting. Communications of the ACM, 45(12), 38–44.
17. Kohno,T.,Stubblefield, A.,Rubin, A.D.,& Wallach, D.S.(2004). Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy, 27(2), 27–40.
18. Neumann,P.G.(1993).Security Criteria for Electronic Voting. Proceedings of the 16thNational Computer Security Conference, 553–559.
19. Mercuri, R.(2001). Electronic Vote Tabulation: Checks and Balances. IEEE Computer, 34(3), 51– 57.
20. Cetinkaya,O.,& Cetinkaya,D.(2007). A Secure Online Voting System Using Homomorphic Encryption. Proceedings of the 2007 International Symposium on Computer Networks.
21. Cranor,L.F.,&Cytron,R.K.(1997). Design and Implementation ofa Secure Online Voting System. IEEE Symposium on Security and Privacy, 88–99.
22. Adams, A., & Laurie, B. (1999). Security of Electronic Voting Systems. Software Engineering Notes, 34(1), 18–26.
23. Simons,B.,&Jones,D.W.(2004).InternetVoting in Public Elections: A Research Perspective on Current Developments. ACM Transactions on Internet Technology, 4(3), 217–238.
24. Cranor,L.F. (1996).Electronic Voting. Communications of the ACM.