Ensuring the Integrity of Online Votes

Berline Najacque

Old Dominion University

Cyber Election Security

Research Paper

Malik A Gladden

August 3, 2024

Ensuring the Integrity of Online Votes

Introduction

Globalization, digitalization, industrialization, and smart technologies have changed the way democratic processes view the traditional voting system. There was a dire need for the online voting system to uphold national integrity. Organizations utilize multiple methodologies to ensure a fair electoral process. As the process increasingly incorporates digital components, the security of digital voting has become more critical yet important over time. Expanding on the identified challenges and solutions, the paper explores resources, tools, and frameworks related to the cyber security of digital voting.

Overview of the Research

People had to face different limitations in the efficiency and security of the voting process before the advent of the online voting system. Still, it became more complicated with increased data breaches as digital voting became popular. However, it has also minimized the pre-existing limitations while ensuring greater convenience, efficiency, and security of the people’s right to vote. The research involves the evaluation of the effectiveness of different security measures that are used to examine threats, including phishing, hacking, or data manipulation (Gritzalis, 2002). It also emphasizes system transparency, voter identification, and cyber threat identification to ensure the process's integrity and security. Overall, the research reviews the best practices, including multi-factor authentication, data encryption, and secure software development, to help evaluate the vulnerabilities within the online voting infrastructure.

Frameworks/Methodology

For risk assessment and management, the stakeholders must ensure end-to-end verifiability and implement security protocols for fair voting. Regular audits, risk mitigation assessments, and adequate education or training on the latest best practices for online voting can also enhance integrity and security. Implementing multi-factor authentication, such as biometrics, helps the stakeholders adopt the NIST cybersecurity framework. This framework helps to identify, protect, detect, respond to, and recover the vulnerabilities in online voting systems. Moreover, tools like the “Election Security Risk Profile Tool” ensure end-to-end verifiability through risk assessment and management so that the voter can verify each vote without compromising the anonymity of any individual involved in the voting process. Developing systems to conduct regular audits allows for the identification of threats. Providing continuous training for election officials and other stakeholders will ensure that every alteration is easily detectable, preventing tampering and ensuring transparency (*How Can U.S. Electronic Voting Systems Be Made More Secure*, 2022). These frameworks evaluate the likelihood, scale, and severity of potential attacks and prioritize mitigation efforts accordingly to reduce unauthorized access and enhance security.

Resources/Results

The logging mechanisms allow for comprehensive audit trails in order to track all actions for verification and identification purposes within the voting system. The extensive "Election Security Risk Profile" tool helps stakeholders assess and prioritize risks. Besides, voter education programs and training educate voters about the importance of cybersecurity and how to protect voters’ information when voting through digital means. The AES (Advanced Encryption Standards) and cryptographic algorithms ensure that votes are securely transmitted and safely stored before any individual, agency, or political party can exploit them. This cybersecurity

toolkit of standards and algorithms offers a collection of services to enhance the cyber resilience of election infrastructure. For instance, multi-factor authentication has reduced the risk of potential cyber threats, unauthorized access, and data breaches. Moreover, the NIST guideline provides a roadmap for local election officials and stakeholders to prepare for and respond to cyber threats so that significant improvements in the resilience and security of the online voting system can be made ("Election Security," 2022).

Conclusion

Maintaining the integrity of online voting is a complex challenge that requires a combination of robust methodologies, advanced technologies, and complete vigilance so that voting officials can significantly enhance the security of the electoral voting system. Implementing principles and methodologies, including end-to-end verifiability, comprehensive risk management, and following NIST guidelines, is essential. Through these, one can significantly enhance the trustworthiness of the digital electoral process and also ensure the resilience of the democratic process.

References

Election Security. (2022). *NIST*. https://www.nist.gov/itl/voting/research-and-projects/election-security

Gritzalis, D. A. (2002). Principles and requirements for a secure e-voting system. *Computers & Security*, *21*(6), 539–556.

How Can U.S. Electronic Voting Systems Be Made More Secure? | Tufts Now. (2022, November 4). https://now.tufts.edu/2022/11/04/how-can-us-electronic-voting-systems-be-made-more-secure