1:Blanchard, E., Gallais, A., Leblond, E., Sidhoum-Rahal, D., & Walter, J. (2022, September). An Analysis of the Security and Privacy Issues of the Neovote Online Voting System. In *International Joint Conference on Electronic Voting* (pp. 1-18). Cham: Springer International Publishing.

**An Analysis of the Security and Privacy Issues of the Neovote Online Voting System**

**Brief Description of the Topic**

The paper delves into a critical examination of the Neovote online voting system, shedding light on the significant security and privacy concerns plaguing this widely utilized platform. Neovote, adopted by numerous companies and institutions for conducting internal elections, has faced scrutiny regarding its susceptibility to vulnerabilities and its failure to ensure the privacy and integrity of the voting process. Through a detailed exploration, the study highlights various flaws within the Neovote system. It elucidates the inadequacies in maintaining the confidentiality of voter information, potential loopholes allowing multiple votes, and the lack of mechanisms to guarantee the integrity of the overall electoral process. The analysis dissects the discrepancies between the system's claimed compliance with regulations and the actual implementation, ultimately calling into question the reliability and trustworthiness of this online voting platform.

The paper rigorously examines Neovote's code structure, revealing instances of code re-use from obsolete libraries and the absence of end-to-end verification processes. These inadequacies not only pose a threat to the privacy of voters but also open avenues for potential attacks that could compromise the legitimacy of the entire voting process. The broader implications of this study reach beyond Neovote's specific issues, advocating for enhanced regulatory frameworks to govern the use of online voting systems. It underscores the necessity for greater transparency, verifiability, and adherence to stringent security standards in technological advancements within democratic processes.This analysis serves as a clarion call for policymakers to reevaluate existing regulations and enforcement mechanisms. It emphasizes the need to prioritize security, privacy, and verifiability in online voting systems to uphold public trust and confidence in democratic practices.

**Conclusions of the Paper**

The study reveals multiple vulnerabilities in Neovote, particularly concerning privacy and security. From inadequate registration procedures to the absence of end-to-end verifiability, the system falls short of ensuring voter privacy and the integrity of the electoral process. The analysis exposes flaws in the code structure, instances of code reuse from outdated libraries, and failures in ensuring end-to-end integrity checks. Moreover, the absence of code transparency and verifiability mechanisms leaves the system susceptible to potential attacks that could compromise the authenticity of the vote.

**Critical Opinion of the Paper**

The paper presents a thorough and critical examination of the Neovote system, highlighting substantial concerns regarding its adherence to established regulations and security best practices. The revelation of code reuse, obsolescent libraries, and the absence of end-to-end verification mechanisms showcases significant vulnerabilities. These vulnerabilities not only compromise the privacy of voters but also cast doubt on the reliability and authenticity of the entire electoral process. The discussion on legal and regulatory constraints underscores the importance of regulatory bodies and enforcement mechanisms to ensure the integrity of online voting systems. The paper rightly advocates for better guidelines and standards to govern the use of such technologies, emphasizing the need for transparency and verifiability to maintain trust in the electoral process.

This analysis serves as a crucial wake-up call for policymakers, urging them to reevaluate existing regulatory frameworks and enforcement mechanisms, ensuring that technological advancements in voting systems prioritize security, privacy, and verifiability. It also underlines the responsibility of for-profit entities like Neovote in upholding stringent security standards, especially when their systems play a critical role in democratic processes. The findings of this paper not only raise serious concerns about the Neovote system but also emphasize the broader need for comprehensive regulations that ensure the integrity of online voting systems, crucial in maintaining public trust and confidence in democratic processes.