EVALUATING THE POTENTIAL IMPLEMENTATION OF REMOTE VOTING SYSTEMS IN UNITED STATES ELECTIONS

by

JOSHUA MARK KIDD

B.A.T., South Texas College, 2021

B.S., New England College, 2023

M.S., Middle Georgia State University, 2023

M.S., Georgia Southwestern State University, 2025

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2026

Evaluating the potential implementation of remote voting systems in United States elections

Joshua Kidd, *Middle Georgia State University, joshua.kidd@mga.edu*

Abstract

Remote voting systems have emerged as a potential solution for improving accessibility and convenience in U.S. elections. However, concerns remain regarding voter anonymity, system dependability, and overall security. This research paper conducted a Systematic Literature Review (SLR) to evaluate cybersecurity vulnerabilities, system failures, and mitigation strategies associated with remote voting technologies. Using databases like IEEE Xplore, Scopus, Google Scholar, and GALILEO, relevant empirical, technical, and policy-based studies were identified and analyzed through thematic synthesis. The findings revealed consistent concerns regarding malware, denial-of-service attacks, and insider threats. Additionally, the absence of voter-verified audit trails limits transparency, recounting capabilities, and independent verification. Although remote voting may increase accessibility for certain populations, the literature indicates that these benefits are modest compared to potential cybersecurity risks. Existing mitigation strategies, including encryption and multi-factor authentication, provide partial safeguards but do not eliminate serious vulnerabilities. Overall, remote voting systems remain technologically and administratively limited, requiring further research and testing.

Keywords: remote voting systems, cybersecurity vulnerabilities, election security, auditability, governance

Introduction

Voting methods in the United States have evolved over time, beginning with the introduction of mechanical voting systems in the 19th century and progressing to electronic voting in the early 21st century. As election systems have become increasingly digitized, concerns regarding election integrity, transparency, and cybersecurity have intensified (Jefferson et al., 2004). These concerns have been amplified by recent controversies surrounding election security and foreign interference.

Unlike traditional in-person or mail-based voting methods, remote voting systems present unique cybersecurity risks due to their reliance on linked digital infrastructures (National Academies of Sciences, Engineering, and Medicine, 2018). The question of whether such systems can be relied upon to maintain both accuracy and anonymity in the electoral process has been raised by these difficulties.

While there are potential advantages to remote voting, like accessibility and convenience, there are also issues with voter anonymity, system dependability, and vulnerabilities.

Therefore, more investigation is necessary to determine if remote voting systems are dependable, provide security, and safeguard election integrity.

Even while voting procedures in the United States have evolved, the advent of remote voting poses new governance and technical difficulties. Although remote voting pilot projects have been put into place in different settings, not much systematic study has been done to assess their security and dependability (Greenhalgh et al., 2018).

Concerns about cybersecurity threats and data integrity in remote voting systems are becoming more prevalent, according to existing literature.

Nevertheless, there remains insufficient publicly verifiable empirical evidence to determine whether remote voting systems consistently uphold constitutional requirements related to ballot secrecy and voter confidentiality, or whether they reliably meet contemporary cybersecurity standards under real-world conditions. (Specter et al., 2020).

This disparity underscores the need for a systematic examination of technological vulnerabilities, risk-mitigation strategies, and legislative frameworks that govern the implementation of remote voting systems in the United States.

This study was guided by the Technology Acceptance Model (TAM), which explains how perceived usefulness and perceived ease of use influence acceptance of emerging technologies. TAM is relevant to remote voting systems because perceptions regarding accessibility, usability, security, and trust may influence public acceptance of internet-based voting technologies, particularly when accessibility benefits conflict with concerns related to cybersecurity vulnerabilities, auditability, governance limitations, and election integrity.

The purpose of this study was to systematically evaluate the vulnerabilities, failures, and mitigation strategies associated with remote voting systems in the United States, and to identify viable solutions for safeguarding electoral integrity.

This research sought to analyze the technical, administrative, and regulatory mechanisms designed to secure these systems, while also exploring their implications for public trust, democratic participation, and technological governance (National Institute of Standards and Technology, 2020; Norden & Famighetti, 2017).

To guide this Systematic Literature Review, the following research questions were developed:

RQ1: How do existing empirical and technical studies characterize the security and resilience of remote voting systems against cybersecurity threats?

RQ2: What specific vulnerabilities and failures have been identified through testing and expert analysis?

RQ3: What mitigation measures have been implemented, and how effective were they?

Review of Literature

Estonia remains the most prominent example of nationwide internet voting implementation, having deployed online voting in national elections since 2005; however, researchers have identified persistent concerns related to system security, endpoint vulnerabilities, and transparency limitations (Ehin et al., 2022; Zhang et al., 2021). Other countries have explored internet voting through limited or pilot programs rather than full-scale implementation.

For example, Switzerland has implemented controlled trials of internet voting, particularly for expatriate voters, but research indicates mixed outcomes and ongoing security concerns (Germann, 2020; Germann & Serdült, 2017). Additional implementations in countries such as Norway and Canada have remained localized or have been discontinued due to security risks and concerns about public trust (International Institute for Democracy and Electoral Assistance, 2023).

Currently, the United States does not utilize nationwide remote internet voting systems for the public when it comes to elections. Limited electronic ballot return systems have been used for certain overseas and

military voters. However, studies and policy analyses consistently caution against broader adoption due to unresolved cybersecurity vulnerabilities, including risks to ballot secrecy, system integrity, and large-scale election manipulation (National Academies of Sciences, Engineering, and Medicine, 2018; Specter & Halderman, 2020; National Conference of State Legislatures, 2023; Verified Voting, 2023).

The increasing use of digital technologies in U.S. elections has sparked a great deal of academic inquiry on the governance, security, and accessibility of remote voting systems. Fundamental issues with voter authentication, ballot secrecy, verification, and transmission integrity in remote-based voting were first noted by Jefferson et al. (2004).

Beyond technical vulnerabilities, this research demonstrated that election systems need security standards that are higher than those of traditional information systems, as they are essential to maintaining democratic legitimacy, because errors in elections that go undetected have particularly dire repercussions (Jefferson et al., 2004).

By placing remote voting within more comprehensive democratic, administrative, and governance contexts, later research broadened the analysis's focus. The National Academies of Sciences, Engineering, and Medicine (2018) and Greenhalgh, Goodman, Rosenzweig, and Epstein (2018) came to the conclusion that while remote voting technologies may improve access for voters who live abroad, military personnel, and people with disabilities, these advantages come with increased vulnerability to malware, DoS (denial-of-service) attacks, insider threats, and foreign interference.

These studies also highlighted how election authorities' capacity to carry out meaningful post-election audits is limited by remote-based systems, which also lack efficient recovery methods in the event of a compromise (Greenhalgh et al., 2018; National Academies of Sciences, Engineering, and Medicine, 2018).

The ongoing trade-off between accessibility and security is a recurring issue in the literature (Horwitz, 2016; Fowler, 2020). Convenience-driven implementations, especially mobile voting trials, frequently stressed usability, while neglecting crucial security measures, according to Horwitz (2016) and Fowler (2020).

Reducing voter friction often increases vulnerability to malware and additional security threats, as illustrated by Fowler (2020). Related turnout-focused studies by Germann (2020), Goodman and Stokes (2018), and Petitpas et al. (2020) indicated that although remote voting might slightly lower voting expenses for certain groups, these benefits are small and do not exceed the overwhelming systemic security threats.

Additionally, emerging technologies have been critically assessed. Blockchain-based voting systems, according to Park, Specter, Narula, and Rivest (2021), do not address fundamental election security issues and may even make them worse by permanently storing tainted or forced votes. This would increase, rather than lessen the impact of attacks.

These concerns were further supported by empirical security evaluations. Researchers at the Massachusetts Institute of Technology found flaws in the Voatz mobile voting system that could jeopardize voter privacy, ballot integrity, and system availability (Specter et al., 2020). Analyses of additional remote voting platforms revealed similar results, showing that end-to-end verifiability is compromised by reliance on internet interfaces, for example. (Specter & Halderman, 2020).

The enduring significance of paper-based voting methods is widely acknowledged in both technical and policy-oriented studies. Despite assertions of encryption and transparency, the American Association for the Advancement of Science (2021) and Appel (2023) contended that most remote voting methods lack verifiability equal to physical ballots.

Voter-verified paper ballots are still necessary for audits, forensic analysis, and recounts, according to Norden and Famighetti (2017) and Tisler and Baker (2022). Public-facing evaluations from Verified Voting (Emerson, 2023) and NPR (Parks, 2023), as well as security standards and guidelines from the National Institute of Standards and Technology (2020), support this consensus by concluding that remote voting remains insecure at scale.

The literature collectively demonstrates widespread consensus that the viability of remote voting technologies in the United States is still hampered by unresolved cybersecurity threats (National Academies of Sciences, Engineering, and Medicine, 2018; Norden & Famighetti, 2017; Tisler & Baker, 2022). The methodical integration of technological security discoveries with governance, regulatory compliance, and administrative viability, however, continues to be lacking. Few studies thoroughly combine these fields, even though current research offers insightful theoretical analysis, case studies, and policy assessments.

Methodology

This study employed a Systematic Literature Review as its primary research methodology to examine existing research about remote voting, governance frameworks, regulatory oversight, election security, cybersecurity threats, and election system vulnerabilities.

The SLR methodology was chosen because it offers a transparent, replicable, and rigorous framework to identify, evaluate, and integrate results from multiple sources (Snyder, 2019). The SLR process adhered to accepted methodological guidelines for transdisciplinary and information systems systematic reviews (Xiao & Watson, 2019).

To guarantee transparency and consistency, the review protocol predetermined research questions, located pertinent databases, set inclusion and exclusion criteria, and documented the screening and extraction processes. This structured approach ensured methodological rigor and alignment with accepted SLR standards.

Inclusion Criteria:

- Use peer-reviewed journal articles, government reports, technical security analyses, or standards publications.
- Address remote voting systems or internet/mobile voting in the United States or comparable democratic contexts.
- Examine cybersecurity vulnerabilities, governance implications, auditability, or mitigation strategies.
- Sources must have been published within the previous ten years, unless considered foundational.

Exclusion Criteria eliminated:

- Opinion pieces that lack empirical or technical grounding.
- Studies unrelated to election security or governance.
- Duplicate publications or sources that cannot be verified.

Literature Search Strategy

A structured literature search was conducted across multiple academic databases, such as IEEE Xplore, Google Scholar, GALILEO, and Scopus. Search queries were constructed using Boolean search strings to maximize retrieval sensitivity while maintaining relevance.

Example Boolean search strings included:

("remote voting" OR "internet voting" OR "mobile voting") AND ("cybersecurity" OR "security vulnerabilities" OR "election security") AND ("verification" OR "governance" OR "risk mitigation").

The literature search was limited to studies published between 2016 and 2026, with earlier foundational works included where necessary. This timeframe was chosen to highlight any recent advancements in cybersecurity, digital infrastructure, and remote voting technologies (Xiao and Watson, 2019).

Data Sources

Data were collected from scholarly databases and academic search engines, including Galileo and Google Scholar. These sources were chosen because thorough database coverage is necessary for systematic reviews to reduce publication bias and guarantee widespread retrieval of relevant studies (Snyder, 2019).

The review included peer-reviewed journal articles, government reports, standards publications, and technical security analyses published within the previous ten years. Sources were required to address one or more of the following subjects:

- Remote Voting Systems
- Election Cybersecurity
- Election Governance
- Regulatory Compliance
- Voting System Auditing

To improve retrieval sensitivity while preserving relevance, several search terms and Boolean combinations were employed in accordance with SLR best practices (Xiao & Watson, 2019).

Screening and Study Selection Procedures

As part of the SLR, a systematic, multi-phase screening process was used for the literature screening process (Xiao & Watson, 2019).

The predefined keywords that were used in the first database searches pertained to:

- Remote Voting
- Internet Voting
- Mobile Voting
- Cybersecurity
- Security Vulnerabilities
- Election Security
- Governance

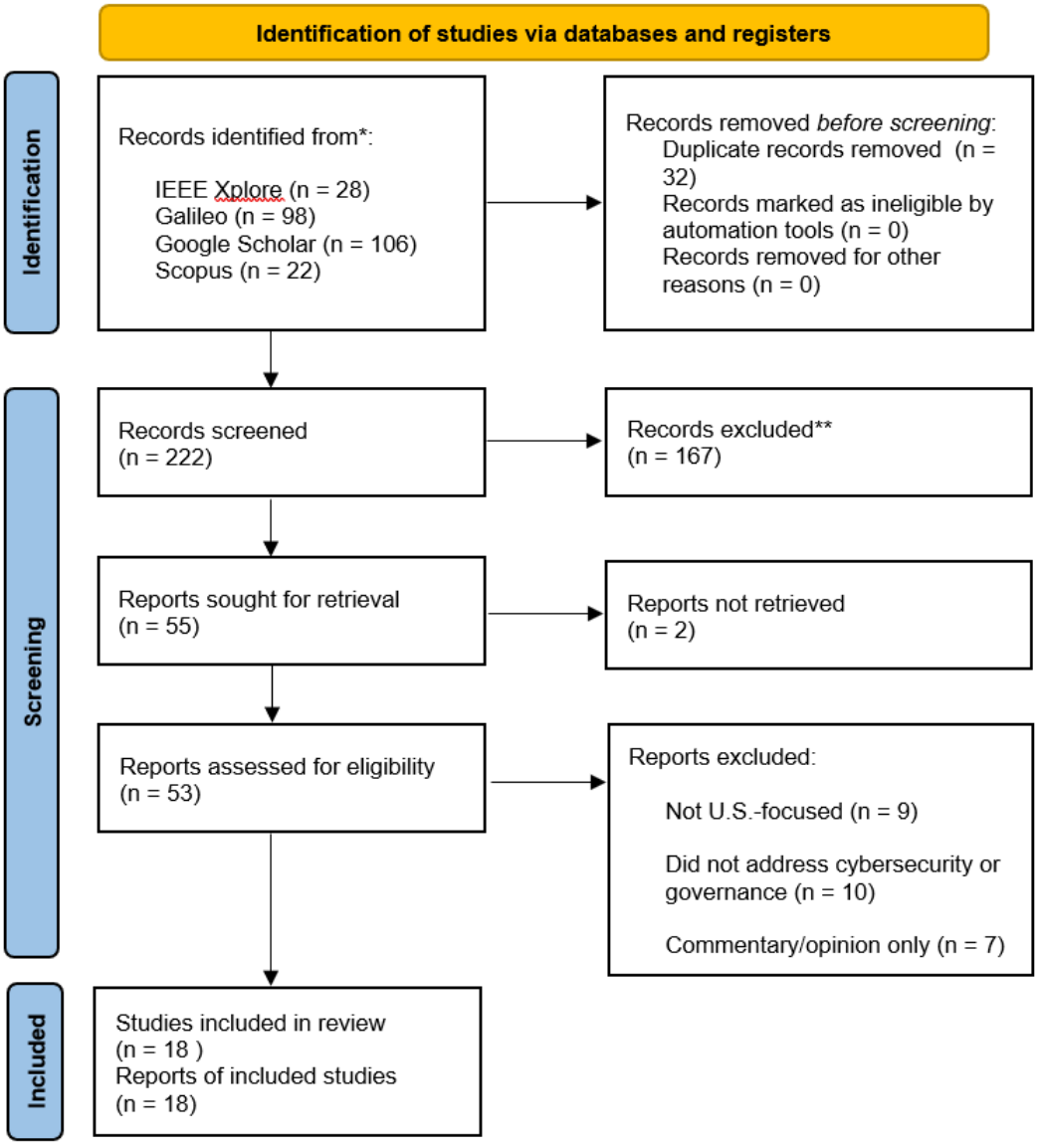
After reviewing titles and abstracts to determine their applicability, full-text analysis was conducted to verify eligibility.

Excluded studies were those that did not fit the inclusion criteria or had no significant bearing on election security or governance.

PRISMA Flow Diagram

The study selection process was documented using the PRISMA 2020 Flow Diagram (Page et al., 2021), outlining identification, screening, eligibility, and inclusion stages.

Figure 1: PRISMA 2020 Flow Diagram of Study Selection Process



Note. Adapted from Page et al. (2021).

The study selection process is illustrated in Figure 1, following PRISMA 2020 guidelines (Page et al., 2021), and outlines the identification, screening, eligibility, and inclusion stages.

Data Extraction

A standardized extraction matrix was used to code the eligible studies in a methodical manner (Snyder, 2019). The extraction framework included the following factors:

- Voting System Type
- Identified Threat Vectors
- Risk Categories
- Mitigation Techniques
- Governance or Regulatory Implications
- Auditability Characteristics
- Study Methodology
- Evidence Type

The extraction process was conducted using Microsoft Excel to organize and systematically compare data across studies. This method improved cross-study comparability and ensured consistency in the application of extraction criteria.

Thematic Coding

Thematic coding was used after extraction to find recurring patterns across various studies. The extraction matrix's initial codes were examined and categorized into more comprehensive conceptual groups that matched the study topics (Braun & Clarke, 2006; Nowell et al., 2017; Saldaña, 2021). Higher-order topics, such as cybersecurity vulnerabilities, auditability constraints, accessibility trade-offs, governance issues, and mitigation techniques, were formed by iteratively comparing similar scripts. This procedure made sure that rather than reflecting isolated findings, the final thematic structure represented recurring patterns found in all the included investigations (Snyder, 2019).

Coding Process

The coding process followed established qualitative synthesis techniques, including thematic analysis and constant comparative methods (Nowell et al., 2017; Saldaña, 2021). Coding activities were supported using Microsoft Excel to organize and refine coded data. An initial open coding phase was conducted to identify recurring concepts across studies. Codes were then grouped into categories using axial coding to establish relationships among variables (Saldaña, 2021). Finally, selective coding was applied to refine overarching themes aligned with the research questions. This iterative process ensured analytical rigor, consistency, and traceability across studies (Snyder, 2019).

Data Analysis

Thematic synthesis was used to evaluate the extracted data (Snyder, 2019; Xiao & Watson, 2019). Cybersecurity vulnerabilities, governance issues, regulatory limitations, and the efficacy of mitigation were

shown to be recurring themes throughout research. The effectiveness of various voting systems in addressing comparable threat profiles and the alignment of suggested protections with accepted election security principles were assessed through comparative analysis. Through this implemented SLR process, the study systematically examined remote voting systems using existing empirical findings, policy analyses, and cybersecurity research.

Summary of Included Studies

Table 1: Summary of Included Studies

Citation	Study Type	Focus	Key Findings
Jefferson et al. (2004)	Technical Analysis	Internet Voting	Fundamental Vulnerabilities
Horwitz (2016)	Policy Reporting	Online Voting	Security Concerns Widespread
Norden and Famighetti (2017)	Policy Analysis	Paper Ballots	Paper Improves Auditability
Goodman and Stokes (2018)	Security Audit	Internet Voting	Minimal Turnout Impact
Greenhalgh et al. (2018)	Security Analysis	E-Mail/Internet Voting	Malware and Interference Risks
Fowler (2020)	Policy Analysis	Mobile Voting	Security Trade-Offs
Germann (2020)	Empirical Study	Voter Turnout	Limited Accessibility Benefits
Petitpas et al. (2020)	Empirical Study	E-Voting Turnout	Limited Participation Benefits
Specter et al. (2020)	Security Audit	Mobile Voting	Critical Integrity Flaws
Specter and Halderman (2020)	Security Analysis	OmniBallot	Ballot Tampering Risks
Park et al. (2021)	Cryptographic Analysis	Blockchain voting	Blockchain Does Not Resolve Security Risks
Tisler and Baker (2022)	Policy Analysis	Election Security	Paper Ballots Enhance Election Integrity
Appel (2023)	Policy Analysis	Internet Voting	Lack Of Verifiability Identified
Emerson (2023)	Policy Evaluation	Election Governance	Internet Voting Threats Persist
Parks (2023)	Policy Reporting	Online Voting	Risk At Scale Remains Significant

Results

This section presents the findings of the systematic literature review, organized according to the research questions guiding the study.

RQ1: How do existing empirical and technical studies characterize the security and resilience of remote voting systems against cybersecurity threats?

As it relates to RQ1, the findings indicated that remote voting systems were consistently characterized as vulnerable to cybersecurity threats, including malware and denial-of-service attacks (Specter et al., 2020).

RQ2: What specific vulnerabilities and failures have been identified through testing and expert analysis?

In assessing RQ2, the findings demonstrated that endpoint compromise, insider threats, and lack of auditability were the most frequently identified vulnerabilities.

RQ3: What mitigation measures have been implemented, and how effective were they?

With respect to RQ3, the results showed that encryption and multi-factor authentication provided partial protection but did not eliminate core vulnerabilities.

Following the responses to the research questions, the results were further organized into thematic categories derived from the systematic analysis of literature.

The thematic synthesis revealed not only recurring patterns across studies, but also a convergence of findings across technical, empirical, and policy-oriented research.

Across all categories, the findings demonstrated that vulnerabilities are systemic rather than incidental, as current technological solutions do not adequately address fundamental security limitations in remote voting systems.

The systematic review consistently identified concerns related to the security, auditability, governance, and technological reliability of remote voting systems in the United States.

Across empirical studies, technical security analyses, and policy evaluations, remote voting was found to slightly enhance voter accessibility, yet significant cybersecurity and verification risks remain unresolved. The findings below were organized into major themes derived from thematic synthesis.

Table 2: Themes, Key Findings, Challenges, Sources, and Number of Studies

Theme	Key Findings	Challenges	Sources	Number of Studies
Cybersecurity Vulnerabilities	Remote voting systems are structurally susceptible to malware, denial-of-service attacks, insider threats, and endpoint compromise. Empirical analyses reveal exploitable vulnerabilities in internet and mobile voting platforms, and blockchain solutions do not eliminate foundational risks.	Structural vulnerabilities persist due to reliance on unsecured personal devices and internet infrastructure. Detection and prevention mechanisms remain insufficient.	Jefferson et al. (2004); Specter et al. (2020); Specter & Halderman (2020); National Academies (2018); Park et al. (2021)	**5**

Auditability and Verification Limitations	Remote systems lack voter-verifiable paper audit trails, significantly limiting recounts, independent verification, and forensic review compared to paper-based systems.	Reduced transparency and diminished ability to detect or correct compromise increase systemic governance risk.	Norden & Famighetti (2017); Tisler & Baker (2022); American Association for the Advancement of Science (2021); Greenhalgh et al. (2018)	**4**
Accessibility versus Security Trade-Off	Remote voting may modestly increase participation for certain populations, particularly overseas voters and individuals with disabilities.	Increased convenience expands attack surfaces and weakens security safeguards. Accessibility gains remain limited relative to systemic risk.	Germann (2020); Goodman & Stokes (2018); Horwitz (2016); Fowler (2020)	**4**
Governance and Regulatory Challenges	Election systems require higher security standards than traditional IT environments due to the irreversible consequences of compromise. Current regulatory frameworks provide guidance but are insufficient for secure nationwide deployment.	Governance gaps, inconsistent standards, and limited institutional capacity complicate oversight and large-scale implementation.	National Academies (2018); National Institute of Standards and Technology (2020); Emerson (2023); Parks (2023)	**4**
Mitigation Strategies and Their Limitations	Encryption, multi-factor authentication, and cryptographic auditing provide partial safeguards that may reduce certain risks.	Mitigation strategies do not eliminate endpoint compromise, coercion risks, insider threats, or core architectural vulnerabilities.	Park et al. (2021); Specter et al. (2020); Jefferson et al. (2004)	**3**

Cybersecurity Vulnerabilities in Remote Voting Systems

Remote voting systems are consistently characterized as structurally vulnerable to malware, denial-of-service attacks, insider threats, and insecure endpoint devices (Jefferson et al., 2004; Specter et al., 2020; Specter & Halderman, 2020). National-level assessments conclude that blockchain enhancements and other technological safeguards do not fully mitigate these risks (National Academies of Sciences, Engineering, and Medicine, 2018; Park et al., 2021). Across multiple studies, these vulnerabilities are described as inherent to internet-based architecture, rather than temporary design flaws.

Auditability and Verification Limitations

A central concern identified across studies is the absence of voter-verifiable audit trails in remote voting systems. Without physical ballots, meaningful recounts and independent verification are significantly constrained (Norden & Famighetti, 2017; Tisler & Baker, 2022). Scholars argue that these limitations reduce transparency and weaken the ability to detect or correct compromise, thereby increasing governance-level risk (Greenhalgh et al., 2018; American Association for the Advancement of Science, 2021).

Accessibility Benefits Versus Security Trade-Offs

Although remote voting may modestly improve participation for certain populations (Germann, 2020; Goodman & Stokes, 2018), researchers consistently observe that increased convenience expands attack surfaces and weakens security safeguards (Horwitz, 2016; Fowler, 2020). The literature broadly concludes that accessibility gains do not outweigh systemic cybersecurity and auditability risks.

Governance and Regulatory Challenges

Election systems require security standards that exceed those of conventional IT environments due to the irreversible consequences of compromised ballots (National Academies of Sciences, Engineering, and Medicine, 2018; National Institute of Standards and Technology, 2020). However, existing regulatory frameworks and institutional capacities appear insufficient to securely manage large-scale remote voting implementation (Greenhalgh et al., 2018; Emerson, 2023). Governance limitations therefore amplify technical vulnerabilities.

Mitigation Strategies and Their Limitations

While encryption, multi-factor authentication, and cryptographic auditing mechanisms provide partial safeguards, they do not eliminate endpoint compromise, coercion risks, or insider threats (Jefferson et al., 2004; Park et al., 2021; Specter et al., 2020). The consensus across studies indicates that mitigation strategies may reduce risk but do not resolve underlying architectural vulnerabilities.

Comparison of Key Results

Table 3: Comparison of Key Results

Study	System Type	Key Vulnerability	Mitigation Proposed	Outcome
National Academies of Sciences, Engineering, and Medicine (2018)	Internet Voting	Systemic Cyber Threats	Policy Recommendations	Not Secure At Scale
Specter et al. (2020)	Mobile Voting (Voatz)	Malware, Privacy Risks	Encryption, App Security	Insufficient

Specter and Halderman (2020)	OmniBallot	Ballot Tampering Risk	Web-Based Protections	Vulnerable
Park et al. (2021)	Blockchain Voting	Immutable Compromised Votes	Cryptographic Verification	Ineffective

The following discussion interprets these findings and examines their broader implications for remote voting systems.

Summary of Findings

The thematic synthesis reflects broad scholarly consensus that remote voting technologies in the United States present persistent cybersecurity, auditability, and governance challenges (National Academies of Sciences, Engineering, and Medicine, 2018; Specter et al., 2020; Park et al., 2021). Although accessibility benefits are acknowledged, empirical evaluations consistently reveal structural vulnerabilities that undermine resilience against cyber threats (Germann, 2020; Fowler, 2020). Current mitigation strategies do not provide security equivalence to traditional paper-based systems, indicating that remote voting remains technologically and administratively constrained (Norden & Famighetti, 2017; Tisler & Baker, 2022).

Discussion and Implications of Findings

The findings of this systematic literature review reveal consistent patterns across empirical, technical, and policy-oriented studies. The findings indicate that remote voting systems face structural cybersecurity vulnerabilities, including malware risks, denial-of-service attacks, insider threats, and endpoint compromise (Jefferson et al., 2004; Specter et al., 2020; Specter & Halderman, 2020).

These risks are inherent to internet-based architectures and remain difficult to fully mitigate, aligning with prior research that consistently characterizes remote voting systems as insecure at scale (National Academies of Sciences, Engineering, and Medicine, 2018; American Association for the Advancement of Science, 2021).

Auditability limitations also emerged as a central concern. Without voter-verified paper audit trails, election officials face challenges conducting recounts, forensic investigations, and independent verification (Norden & Famighetti, 2017; Tisler & Baker, 2022). These findings align with prior research emphasizing that paper-based systems remain essential for ensuring transparency and election integrity (American Association for the Advancement of Science, 2021; Appel, 2023).

Additionally, while remote voting may improve accessibility for certain populations, studies indicate that participation gains are modest and may not outweigh the increased cybersecurity risks (Germann, 2020; Goodman & Stokes, 2018). Governance and regulatory challenges further complicate remote voting implementation, as existing frameworks often lack the capacity to ensure secure large-scale deployment; existing standards emphasize the importance of risk management and system security controls (National Institute of Standards and Technology, 2020; Emerson, 2023; Parks, 2023).

Across studies, remote voting systems are widely characterized as lacking sufficient safeguards to ensure election integrity at scale. This indicates that technological and administrative limitations remain unresolved (National Academies of Sciences, Engineering, and Medicine, 2018; Park et al., 2021).

The findings of this study have important implications for policymakers, election administrators, and cybersecurity professionals. The persistent vulnerabilities identified across studies suggest that remote voting systems should be implemented cautiously and only in limited contexts.

The findings also highlight the importance of maintaining voter-verified paper ballots and auditable election systems (Norden & Famighetti, 2017; Tisler & Baker, 2022).

These safeguards remain essential for ensuring transparency, accountability, and public trust (Verified Voting, 2023). Additionally, governance frameworks and regulatory standards should be strengthened to address emerging cybersecurity threats (National Institute of Standards and Technology, 2020; American Association for the Advancement of Science, 2021).

Overall, the findings emphasize that election security and integrity should remain as primary considerations when evaluating remote voting technologies. Until these challenges are adequately addressed, remote voting systems remain constrained by both technical and governance limitations.

Conclusion

This research paper examined the security, auditability, governance, and technological challenges associated with remote voting systems in the United States. The findings indicate that remote voting systems continue to experience persistent security risks and governance limitations.

Although remote voting offers potential accessibility benefits, these advantages appear limited when compared to the risks associated with cybersecurity threats and system compromise. Current mitigation strategies provide partial safeguards but do not eliminate structural vulnerabilities.

Remote voting remains a developing technology that requires further research, testing, and governance improvements before widespread implementation.

In addition to these findings, this research paper is subject to several limitations. First, the systematic literature review relied on publicly available academic and policy sources, which may not capture all potential vulnerabilities or proprietary security assessments. Second, the review focused primarily on studies conducted within the United States or comparable democratic contexts, which may limit generalizability.

Additionally, the use of selected databases, including IEEE Xplore, Scopus, Google Scholar, and GALILEO, may have excluded relevant studies.

The rapidly evolving nature of technology and cybersecurity may limit the long-term applicability of findings. Emerging technologies and evolving threat landscapes may influence the security and viability of remote voting systems over time, requiring continued research, testing, and evaluation.

Building on these limitations, future research should focus on evaluating emerging remote voting technologies through empirical testing and pilot implementations. Controlled pilot studies may provide valuable insights into system performance, usability, and security vulnerabilities under real-world conditions.

Additionally, future research should examine advanced cryptographic techniques, including end-to-end verifiable voting systems, to determine whether these approaches can improve remote voting security. Further analysis of blockchain-based voting technologies should also be conducted, particularly regarding coercion resistance, endpoint security, and auditability.

Research is also needed to examine governance frameworks and regulatory approaches for remote voting implementation. Studies exploring risk management, compliance standards, and oversight mechanisms may contribute to improved election security policies and administrative practices.

Another important area for future research involves accessibility outcomes. Additional empirical studies should evaluate whether remote voting significantly improves participation among certain populations and whether these benefits outweigh potential cybersecurity risks.

Finally, interdisciplinary research involving cybersecurity, public policy, election administration, and information technology is recommended. Collaborative research approaches may help identify balanced solutions that address accessibility concerns while maintaining election integrity.

References

American Association for the Advancement of Science. (2021). *Internet or online voting remains insecure*. https://www.aaas.org/epi-center/internet-online-voting

Appel, A. (2023). Is internet voting trustworthy? The science and the policy battles. *University of New Hampshire Law Review, 21*(2). https://scholars.unh.edu/unh_lr/vol21/iss2/9/

Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. Government Information Quarterly, 39(4), 101718. https://www.sciencedirect.com/science/article/pii/S0740624X2200051X

Emerson, B. C. (2023, March 24). Why internet voting is a threat to our democracy. *Verified Voting*. https://verifiedvoting.org/why-internet-voting-is-a-threat-to-our-democracy/

Fowler, A. (2020, September 17). Promises and perils of mobile voting. *Election Law Journal: Rules, Politics, and Policy, 19*(3). https://doi.org/10.1089/elj.2019.0589

Germann, M., & Serdült, U. (2017). Internet voting and turnout: Evidence from Switzerland. Electoral Studies, 47, 1–12. https://doi.org/10.1016/j.electstud.2017.03.001

Germann, M. (2020). Making votes count with internet voting. *Political Behavior, 43*(4), 1511–1533. https://doi.org/10.1007/s11109-020-09598-2

Goodman, N., & Stokes, L. C. (2018). Reducing the cost of voting: An evaluation of internet voting's effect on turnout. *British Journal of Political Science, 50*(3), 1155–1167. https://doi.org/10.1017/s0007123417000849

Greenhalgh, S., Goodman, S., Rosenzweig, P., & Epstein, J. (2018). *Email and internet voting: The overlooked threat to election security*. Association for Computing Machinery. https://www.acm.org/binaries/content/assets/public-policy/jtreportemailinternetvoting.pdf

Horwitz, S. (2016, May 17). More than 30 states offer online voting, but experts warn it isn't secure. *The Washington Post*. https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/

International Institute for Democracy and Electoral Assistance. (2023). Use of e-voting around the world. https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world

Jefferson, D., Rubin, A. D., Simons, B., & Wagner, D. (2004). Analyzing internet voting security. *Communications of the ACM, 47*(10), 59–64. https://doi.org/10.1145/1022594.1022624

National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the vote: Protecting American democracy*. The National Academies Press. https://doi.org/10.17226/25120

National Conference of State Legislatures. (2023). Electronic ballot return and internet voting. https://www.ncsl.org/elections-and-campaigns/electronic-ballot-return-internet-voting

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5, Update 1)*. U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Norden, L., & Famighetti, C. (2017, May 10). *The voting technology we really need? Paper*. Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/voting-technology-we-really-need-paper

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13. https://doi.org/10.1177/1609406917733847

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McGuinness, L. A., Stewart, L. A., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From internet voting to blockchain voting. *Journal of Cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyaa025

Parks, M. (2023, September 8). Voting online is very risky. But hundreds of thousands of people are already doing it. *NPR*. https://www.npr.org/2023/09/07/1192723913/internet-voting-explainer

Petitpas, A., Jaquet, J. M., & Sciarini, P. (2020). Does e-voting matter for turnout, and to whom? *Electoral Studies, 71*, 102245. https://doi.org/10.1016/j.electstud.2020.102245

Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE Publications.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Specter, M., Koppel, J., & Weitzner, D. (2020). *The ballot is busted before the blockchain: A security analysis of Voatz, the first internet voting application used in U.S. federal elections*. Massachusetts Institute of Technology. https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

Specter, M. A., & Halderman, J. A. (2020, June 7). *Security analysis of the Democracy Live OmniBallot online voting system*. MIT Internet Policy Research Initiative. https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf

Tisler, D., & Baker, T. (2022, May 10). Paper ballots helped secure the 2020 election — What will 2022 look like? *Brennan Center for Justice*. https://www.brennancenter.org/our-work/analysis-opinion/paper-ballots-helped-secure-2020-election-what-will-2022-look

Verified Voting. (2023). Electronic ballot return is dangerously insecure. https://verifiedvoting.org/publication/electronic-ballot-return-2023/

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Zhang, R., Teague, V., & Culnane, C. (2021). Analysis of the IVXV internet voting system used in Estonia. arXiv. https://arxiv.org/abs/2109.01994