# Digital Voting Systems

Godapitiya Hewage Buddhini Chathurika Gunawardhana

MSc thesis
December 2025

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

**Reviewers:**
Prof. Ion Petre
Ph.D. Yury Nikulin

UNIVERSITY OF TURKU, Department of Mathematics and Statistics

MSc Thesis
**Subject:** Mathematics
**Author:** Godapitiya Hewage Buddhini Chathurika Gunawardhana
**Title:** Digital Voting Systems
**Supervisor:** Prof. Ion Petre
**Pages:** 50 pages
**Month and year:** December 2025

---

**Abstract**

Digital voting systems represent a significant evolution in the democratic process, offering the potential to improve accessibility, efficiency, and transparency in elections. Despite technological advances, widespread adoption remains limited due to concerns about security, usability, and practical deployment. This thesis examines three prominent digital voting systems — Helios, Estonian i-Voting, and Voatz — to assess their readiness for large-scale democratic use.

The research addresses key questions regarding the security and cryptographic robustness, usability and accessibility, and practical deployment characteristics of these systems. A qualitative comparative case study methodology is employed, drawing on published literature, technical documentation, security audits, and real-world deployment reports. Each system is analysed across multiple dimensions, including privacy, integrity, verifiability, coercion resistance, voter experience, infrastructure requirements, and operational performance.

Findings highlight that while each system demonstrates innovative solutions to digital voting challenges, significant trade-offs exist between security, usability, and scalability. Helios provides strong theoretical guarantees and transparency in organizational elections, but practical usability remains a concern. Estonian i-Voting demonstrates the feasibility of national-scale internet voting supported by robust digital identity infrastructure, yet concerns about coercion and system transparency persist. Voatz illustrates the potential of mobile blockchain-based voting but faces critical security vulnerabilities and limited public trust.

This study contributes a systematic, multi-dimensional comparison of digital voting systems, providing insights for policymakers, election administrators, and researchers. By evaluating existing implementations in terms of security, usability, and deployment readiness, the thesis informs future development and adoption strategies for digital voting technologies.

Keywords: Digital Voting, E-Voting Systems, Helios, Estonian i-Voting, Voatz.

# Contents

# 1 Introduction

## 1.1 Background and Motivation

Democracy has always depended on one central act: voting. From the assemblies of ancient Greece to today's modern representative democracies, voting has been the way citizens express their political will and influence governance [22]. As societies move further into the digital age, the traditional paper-based ballot is increasingly being reconsidered. Technological innovations now offer the possibility of elections that are more efficient, more accessible, and potentially more transparent [4].

Digital voting constitutes one of the most significant advancements in the electoral process since the late nineteenth century, when mechanical voting machines were first introduced [4]. These systems use cryptographic methods, secure networks, and user-friendly interfaces to allow citizens to cast their votes electronically [5]. This can take place through dedicated machines in polling stations or remotely via internet-connected devices. The potential benefits are significant. Benefits include lower administrative costs, quicker result tabulation, enhanced accessibility for citizens with disabilities or those residing in remote areas [6], and, in certain cases, increased transparency facilitated by cryptographic verification [4].

In recent years, the impetus to adopt digital voting has intensified due to several converging trends [26]. Younger generations, familiar with digital services in nearly every aspect of life, increasingly anticipate that government services, including voting, will be accessible digitally [26]. At the same time, concerns about election security and integrity have encouraged interest in systems that can provide verifiable guarantees of privacy and correctness [9]. Digital voting is not simply a matter of convenience or modernization. For groups such as military personnel stationed abroad, expatriates, or citizens with mobility limitations, these systems can provide genuine access to democratic participation [30].

Several countries have experimented with or adopted digital voting with varying levels of success. Estonia is the most prominent example, having conducted internet voting in legally binding elections since 2005. The system has processed over 1.9 million votes across multiple election cycles, demonstrating that digital voting can work at a national scale [33, 16].Studies show that participation in Estonian i-Voting grew steadily between 2005 and 2015 [33]. The Estonian approach relies on the country's digital infrastructure, including mandatory digital identity cards supported by PKI certificates [31]. Switzerland has also tested digital voting in several cantons. The Geneva internet voting platform, for example, has been used by tens of thousands of voters in federal and cantonal elections [4]. In the United States, digital voting initiatives have been more limited, focusing mainly on overseas military personnel. The Voatz mobile voting platform has been piloted in several states, but it has attracted strong criticism because of identified security vulnerabilities [30].

Research-driven systems have also contributed to the development of the field. Helios, designed by Ben Adida, is widely used for organizational elections and has provided an important testbed for end-to-end verifiable voting protocols [2]. Its use in university elections has highlighted both its value and the difficulties of implementing open-audit systems [3]. Other research projects such as Scantegrity have

demonstrated how paper-based ballots can be combined with cryptographic verification to achieve stronger guarantees of security [12]. Theoretical contributions, including Benaloh's work on verifiable elections, continue to influence the design of modern systems [8].

Despite these advances, the adoption of digital voting remains difficult. Technical, social, and political challenges must be addressed before it can be considered ready for widespread use. From a technical perspective, ensuring the essential requirements of democratic elections—privacy, integrity, verifiability, and resistance to coercion—is highly complex. In traditional paper-based systems, these properties are supported through physical safeguards and human oversight. In digital systems, however, they rely on cryptographic protocols and software implementations that are not easy for ordinary citizens to understand or verify.

Security concerns are perhaps the most significant obstacle. Cyberattacks, malware, and insider threats could undermine electoral confidence if not addressed effectively [9]. Several audits have revealed critical weaknesses in existing systems, such as the Voatz platform, which was found to have multiple attack vectors [30]. Usability is another critical consideration. A voting system must be accessible to all citizens, including the elderly, individuals with disabilities, and those with limited digital literacy. Yet strong security measures often introduce complex verification steps that can confuse or discourage voters [1]. Beyond the technical challenges, trust plays a decisive role. Public acceptance of digital voting varies widely. In some contexts, concerns about surveillance, privacy, and the possibility of manipulation outweigh any potential benefits [4].

## 1.2 Problem Statement

Despite the development and testing of numerous digital voting systems, significant uncertainty remains regarding their security, usability, and readiness for democratic deployment. Existing literature tends to focus either on highly technical analyses aimed at cryptography experts or on broad policy discussions lacking technical depth. As a result, there is a gap in balanced, comparative evaluations that integrate both perspectives to guide policymakers, election officials, and researchers.

In particular, there is limited understanding of how digital voting systems address core election properties such as verifiability, privacy, and resilience against attacks. Although many systems claim to provide these guarantees, their actual security assurances, practical limitations, and performance in real-world conditions are often unclear.

Usability and accessibility remain relatively underexplored, despite the fact that the success of any voting system relies on voter acceptance and effective use. Coercion resistance, especially in the context of remote voting, is also inadequately studied, leaving potential vulnerabilities to vote buying or undue influence. Consequently, a systematic, multi-dimensional evaluation is essential to assess the trade-offs, strengths, and limitations of existing digital voting systems.

## 1.3 Objectives and Research Questions

This thesis aims to provide a comprehensive analysis and comparison of prominent digital voting systems to evaluate their readiness for large-scale deployment in democratic elections. The research is guided by three primary objectives that address the identified gaps in current understanding.

The first objective involves conducting a thorough security analysis of selected digital voting systems, evaluating their implementation of fundamental voting properties including privacy, integrity, verifiability, and coercion resistance. This analysis will identify the cryptographic techniques employed by each system and assess their effectiveness in providing security guarantees under realistic threat models.

The second objective focuses on evaluating and comparing the usability and accessibility characteristics of digital voting systems, examining their suitability for diverse voter populations and identifying potential barriers to adoption or effective use. This assessment will consider both voter-facing interfaces and administrative requirements.

The third objective involves analyzing the practical aspects of digital voting system deployment, including scalability, performance characteristics, infrastructure requirements, and real-world implementation experiences. This evaluation will inform understanding of the feasibility of large-scale adoption.

The research is structured around several key questions:

- **Security and Cryptographic Robustness:** What cryptographic techniques do prominent digital voting systems employ to ensure privacy, integrity, and verifiability? How effectively do these systems resist common attack vectors including malware, network attacks, and insider threats? What assumptions and limitations exist in the security models employed by different systems?
- **Usability and Accessibility:** How do digital voting systems address the needs of diverse voter populations, including elderly users, individuals with disabilities, and those with limited technological experience? What are the cognitive and procedural demands placed on voters by different verification and interaction mechanisms? How do usability requirements conflict with security objectives, and how do different systems resolve these tensions?
- **Practical Deployment Readiness:** What infrastructure requirements and administrative processes are necessary for successful deployment of digital voting systems? How do these systems perform under realistic load conditions and network constraints? What lessons can be learned from real-world deployments regarding system reliability, public acceptance, and operational challenges?
- **Comparative Assessment:** How do prominent digital voting systems compare across security, usability, and practical deployment dimensions? What are the key trade-offs and design decisions that differentiate these systems? Which approaches show the most promise for large-scale democratic elections?

## 1.4 Scope of the Thesis

This thesis focuses on the analysis and comparison of three prominent digital voting systems that represent different approaches to secure electronic voting: Helios, Estonian i-Voting, and Voatz. These systems were selected to provide diverse perspectives on digital voting implementation, ranging from academic research platforms to nationally deployed systems to commercial mobile voting solutions.

Helios was selected as a representative of academic research in end-to-end verifiable voting systems. Developed by Ben Adida and widely used in academic and organizational elections, Helios embodies many of the theoretical principles of cryptographically secure voting while providing practical implementation experience. Its open-source nature and extensive academic analysis make it an ideal subject for detailed technical evaluation.

The Estonian i-Voting system represents the most successful large-scale implementation of internet voting in legally binding elections. With over fifteen years of operational experience and millions of votes cast, it provides unique insights into the practical challenges and solutions for national-scale digital voting deployment. The system's integration with Estonia's comprehensive digital identity infrastructure offers lessons for other jurisdictions considering similar implementations.

Voatz represents the emerging category of blockchain-based mobile voting systems and demonstrates the application of distributed ledger technology to electoral processes. Despite facing significant security criticism, its deployment in actual U.S. elections and focus on mobile accessibility provide important perspectives on modern digital voting approaches and their limitations.

The analysis employs a multi-dimensional framework that evaluates each system across three primary categories: security, usability, and practical deployment. This thesis focuses specifically on the technical and practical aspects of digital voting systems rather than the broader political, legal, or policy implications of their adoption. While these broader considerations are acknowledged as important, they are beyond the scope of this technical analysis. The research does not include experimental security testing or penetration testing of the selected systems. Instead, it relies on published security analyses, academic literature, and publicly available documentation. This approach ensures that the research remains within ethical boundaries while providing comprehensive analysis based on established findings. The thesis does not propose new cryptographic protocols or voting system designs. Rather, it focuses on evaluating and comparing existing implementations to provide insights that can inform future development and deployment decisions.

## 1.5 Methodology Overview

The research employs a qualitative comparative case study methodology, analyzing each selected voting system through multiple lenses to provide comprehensive understanding of their capabilities and limitations. The methodology combines literature review, technical analysis, and comparative evaluation to address the research questions systematically.

Data collection involves comprehensive review of academic literature, technical

documentation, security audit reports, and real-world deployment studies. Primary sources include peer-reviewed publications, system specifications, security analyses, and official reports from election administrators and oversight bodies. The analysis framework applies consistent evaluation criteria across all selected systems, enabling meaningful comparison and identification of relative strengths and weaknesses. This structured approach ensures that the research findings provide actionable insights for stakeholders involved in digital voting system evaluation and deployment decisions.

## 1.6 Thesis Structure

This thesis is organized into seven chapters that systematically address the research objectives and questions. The introduction provides background context, problem definition, research objectives, and scope delineation. The literature review surveys existing research on digital voting systems, cryptographic techniques, security requirements, and implementation challenges. The theoretical framework establishes the analytical foundation for system evaluation, including security properties, threat models, and evaluation criteria.

The methodology chapter details the research approach, system selection rationale, and analytical procedures. The case studies chapter presents detailed analysis of each selected voting system, examining their architecture, security properties, and implementation characteristics. The comparative analysis synthesizes findings from the individual case studies to provide systematic comparison and identify key insights. The discussion and conclusions chapter interprets the research findings, discusses implications for digital voting adoption, and identifies directions for future research. The thesis concludes with comprehensive references and appendices containing supplementary technical details and analysis frameworks.

# 2 Literature Review

## 2.1 Overview of Voting Systems

The evolution from mechanical to electronic voting systems represents more than a technological transition; it embodies a fundamental shift in how democratic societies balance efficiency, security, and public trust. The mechanical lever machines of the early 20th century, while primitive by today's standards, established important precedents for voting system design by prioritizing voter privacy through physical booth isolation and providing immediate feedback through mechanical indicators. The punch-card systems introduced in the 1960s represented the first significant attempt to combine paper-based recording with automated tabulation. These systems, most notably the Votomatic machines, used pre-scored paper cards that voters punched to indicate their choices. While these systems improved counting efficiency and reduced human error in tabulation, they introduced new failure modes including incomplete punches (hanging chads) and multiple punches that became critically important during the 2000 U.S. presidential election controversy [4].

The transition to Direct Recording Electronic (DRE) systems following the Help America Vote Act of 2002 marked a significant acceleration in electronic voting adoption. These systems eliminated paper ballots entirely, storing votes in electronic memory and providing digital interfaces for voter interaction. Early DRE implementations offered significant advantages in terms of ballot flexibility, multilanguage support, and accessibility features for voters with disabilities. However, the absence of voter-verified paper audit trails in many early systems created serious concerns about auditability and public verifiability [28].

The concept of software independence, as articulated by Rivest and Wack (2006), became a central principle in voting system evaluation. Software-independent voting systems are those in which an undetected change or error in software cannot cause an undetectable change or error in election outcome. This principle highlighted the fundamental limitation of paperless electronic voting systems and drove the development of voter-verified paper audit trail (VVPAT) requirements in many jurisdictions. Optical scan systems emerged as a compromise solution that maintained the auditability of paper ballots while providing the efficiency benefits of electronic tabulation. These systems require voters to mark paper ballots using specified methods (typically filling in bubbles or connecting arrows), which are then processed by scanning equipment that interprets the marks and tabulates results. The dual nature of optical scan systems - combining human-readable paper records with machine-readable electronic processing - addresses many of the auditability concerns associated with DRE systems while maintaining operational efficiency [14].

The security model underlying optical scan systems relies on the principle of separating ballot marking from ballot counting. Voters create permanent, human-readable records of their choices that can be examined during recounts or audits, while automated scanning reduces the time and labour required for initial vote counting. This separation enables election officials to verify electronic tallies against paper records when discrepancies are suspected or audits are required.

The fundamental principles underlying secure voting systems have been exten-

sively studied in the academic literature. Benaloh [8] identified the core requirements for verifiable elections, emphasizing the importance of enabling voters to verify that their votes were cast as intended, recorded as cast, and tallied as recorded. These verification requirements form the foundation for end-to-end verifiable voting systems.

## 2.2 Theoretical Foundations of Digital Voting

The theoretical framework for digital voting systems extends beyond basic cryptographic primitives to encompass fundamental questions about the nature of democratic participation and the role of technology in electoral processes [8, 13]. The work of Benaloh (2006) established that verifiable elections must satisfy three distinct but interconnected requirements: cast-as-intended verification (ensuring that voters' intended choices are properly recorded), recorded-as-cast verification (confirming that recorded votes are not altered during processing), and tallied-as-recorded verification (demonstrating that the final tally accurately reflects all recorded votes) [8, 28].

Cast-as-intended verification presents unique challenges in digital voting systems because it requires enabling voters to confirm their vote choices without compromising ballot secrecy [8]. Traditional paper-based voting provides implicit cast-as-intended verification through the physical act of marking a ballot that voters can observe before submission. Digital voting systems must provide equivalent assurance through cryptographic or procedural mechanisms that may not be intuitive to voters [8]. The mathematical foundations of privacy preservation in digital voting systems draw heavily from the theory of secure multi-party computation. The challenge lies in enabling multiple parties (voters, election officials, observers) to jointly compute election results while keeping individual contributions (votes) private. Homomorphic encryption schemes, particularly those based on the discrete logarithm problem, provide the mathematical tools necessary to perform computations on encrypted data without revealing the underlying plaintext values [27].

The Paillier cryptosystem, with its additive homomorphic properties, enables the direct addition of encrypted votes to produce encrypted tallies [27]. This mathematical property is particularly well-suited to voting applications because election results are typically computed through simple addition operations. The security of the Paillier system relies on the computational difficulty of factoring large composite numbers, a problem that is widely believed to be intractable for sufficiently large key sizes [27]. Integrity guarantees in digital voting systems must address both accidental errors and intentional manipulation. Cryptographic hash functions provide fundamental tools for ensuring data integrity by producing fixed-size fingerprints of data that change dramatically with any modification to the input. Merkle trees and other authenticated data structures enable efficient verification of large datasets while maintaining strong integrity guarantees [5].

The concept of end-to-end verifiability represents a significant theoretical advance over traditional auditing approaches. Rather than relying on procedural controls and trusted parties, end-to-end verifiable systems provide mathematical proofs that election results are correct. This approach shifts the trust model from reliance on system

components and operators to reliance on publicly verifiable mathematical properties [2]. Individual verifiability protocols must balance the competing requirements of enabling voters to verify their ballot inclusion while preventing coercion and vote buying. Receipt-based systems typically provide voters with cryptographic commitments or encrypted representations of their votes that can be verified against publicly posted election data. The challenge lies in ensuring that these receipts cannot be used as proof of vote choice to external parties [13]. Universal verifiability extends beyond individual vote verification to enable any interested party to verify the correctness of the overall election process. This typically involves publishing sufficient cryptographic evidence to allow independent verification of key operations including ballot validation, vote tallying, and result computation. The implementation of universal verifiability requires careful attention to the completeness and accessibility of published verification data [8]. Coercion resistance and receipt-freeness represent some of the most challenging theoretical problems in digital voting system design [24]. Traditional polling place voting provides natural coercion resistance through the secret ballot environment and the inability of voters to prove their vote choices to external parties [24]. Remote digital voting systems must provide equivalent protection through cryptographic or procedural mechanisms [24].

The theoretical framework for coercion resistance, as developed by Juels (2005), requires that voters be able to interact with coercers in ways that are indistinguishable from compliant behavior while actually casting their true vote preferences [24]. This requirement is particularly challenging in systems that provide individual verifiability, as verification mechanisms may potentially be exploited by coercers to confirm voter compliance. Receipt-freeness protocols, such as those developed by Delaune (2009), require that voters cannot generate convincing proof of their vote choices even if they wish to do so. This property helps prevent vote buying by eliminating the ability of voters to demonstrate their compliance with purchaser demands. The implementation of receipt-freeness often requires sophisticated cryptographic protocols that may conflict with usability requirements.

## 2.3 Cryptographic Techniques in Digital Voting

The application of advanced cryptographic techniques to voting systems requires careful consideration of both theoretical security properties and practical implementation constraints. Homomorphic encryption, while providing strong privacy guarantees, introduces computational overhead that must be managed in large-scale election deployments. The exponential ElGamal encryption scheme used in systems like Helios requires careful parameter selection to balance security levels with computational efficiency [2]. The security of ElGamal encryption relies on the discrete logarithm problem in finite fields or elliptic curve groups. For voting applications, the choice of mathematical group significantly impacts both security and performance characteristics. Elliptic curve implementations generally provide equivalent security levels with smaller key sizes, reducing computational and storage requirements. However, the complexity of elliptic curve arithmetic may present implementation challenges that increase the risk of cryptographic vulnerabilities [17]. Zero-knowledge proof systems used in voting applications must satisfy three fun-

damental properties: completeness (honest provers can convince honest verifiers), soundness (dishonest provers cannot convince honest verifiers), and zero-knowledge (verifiers learn nothing beyond the validity of the proven statement). The implementation of these properties in practical voting systems requires careful attention to the specific cryptographic constructions and their security assumptions [20].

Non-interactive zero-knowledge proofs, particularly those generated using the Fiat-Shamir transform, are commonly used in voting systems to avoid the communication overhead of interactive protocols. However, the security of Fiat-Shamir proofs relies on the random oracle model, which may not accurately reflect the security properties of practical hash functions. This gap between theoretical security guarantees and practical implementations represents an ongoing challenge in cryptographic voting system design. Mix networks provide an alternative approach to achieving ballot privacy by breaking the link between voters and their encrypted ballots through cryptographic shuffling. The security of mix networks depends critically on the honest operation of at least one mixing server, creating a distributed trust model that may be more robust than systems relying on single trusted parties. However, the verification of mix network operations requires sophisticated cryptographic proofs that can be computationally expensive for large elections [13]. Verifiable mix networks, as developed by Furukawa and Sako (2001), provide cryptographic proofs that mixing operations were performed correctly without revealing the permutation applied to the input ballots [19]. These proofs enable public verification of mix network integrity while maintaining ballot privacy. The computational complexity of generating and verifying these proofs scales with the number of ballots being mixed, potentially creating performance bottlenecks in large elections. Threshold cryptography addresses the key management challenges inherent in cryptographic voting systems by distributing trust among multiple parties. In threshold decryption schemes, the private key needed to decrypt ballots is shared among multiple trustees using secret sharing techniques. A threshold number of trustees must cooperate to perform decryption operations, preventing any single party from unilaterally accessing ballot contents [29].

The implementation of threshold cryptography in voting systems requires careful attention to key generation ceremonies, trustee selection processes, and key recovery procedures. Key generation ceremonies must ensure that private key shares are distributed securely and that no single party learns the complete private key during the generation process. Trustee selection must balance technical expertise with independence and trustworthiness considerations. Digital signature schemes provide authentication and non-repudiation services in voting systems, enabling the verification of ballot authenticity and system integrity. The Estonian i-Voting system relies heavily on PKI infrastructure, requiring voters to use cryptographic smart cards for ballot signing and authentication. This approach provides strong authentication guarantees but requires comprehensive key management infrastructure and sophisticated end-user devices [31]. The security of PKI-based voting systems depends on the integrity of the entire certificate authority hierarchy and the secure operation of smart card infrastructure. Compromise of certificate authorities or smart card manufacturing processes could undermine the security of the entire voting system. Additionally, the requirement for specialized hardware (smart cards and card read-

ers) may create accessibility barriers for some voters. Blind signature schemes, as introduced by Chaum (1983), provide a mechanism for separating voter authentication from ballot casting. In blind signature protocols, voters can obtain signatures on their ballots without revealing ballot contents to the signing authority. This separation enables voting system architectures that authenticate voter eligibility during one phase of the election process and collect anonymous ballots during a separate phase. The implementation of blind signature schemes in practical voting systems faces several challenges. The blind signature protocols require multiple rounds of communication between voters and signing authorities, potentially creating performance bottlenecks during peak voting periods. Additionally, the prevention of double-voting requires careful protocol design to ensure that voters cannot obtain multiple valid signatures for the same election.

## 2.4 Existing Digital Voting Systems

The landscape of digital voting systems encompasses a diverse range of implementations, from academic research prototypes to commercially deployed systems used in legally binding elections. Examining these implementations provides insights into the practical challenges and trade-offs involved in deploying digital voting technology.

### 2.4.1 Helios Voting System

The Helios voting system represents the most widely studied implementation of end-to-end verifiable voting, with deployments spanning over a decade and encompassing hundreds of elections across diverse organizational contexts. The system's architecture embodies a careful balance between cryptographic rigor and practical usability, though this balance has revealed fundamental tensions between security guarantees and user experience [3]. The cryptographic foundation of Helios rests on exponential ElGamal encryption, which enables homomorphic tallying while maintaining computational efficiency for moderate-scale elections. The choice of exponential ElGamal over standard ElGamal encryption reflects a design decision that prioritizes tallying efficiency over encryption/decryption performance. In exponential ElGamal, vote values are encoded in the exponent of the group generator, enabling direct addition of encrypted votes through group multiplication operations [2].

The zero-knowledge proof system in Helios serves multiple verification purposes simultaneously. Ballot validity proofs demonstrate that encrypted ballots contain legitimate vote choices without revealing the actual votes. These proofs prevent voters from casting invalid ballots that could disrupt the tallying process while maintaining ballot privacy. The implementation uses Chaum-Pedersen proofs for individual candidate selections and disjunctive proofs for ballot validity, striking a balance between proof size and verification efficiency [15]. Individual verifiability in Helios operates through a receipt mechanism that provides voters with cryptographic evidence of ballot inclusion without compromising privacy. Voters receive smart ballot tracker codes that correspond to their encrypted ballots on the public bulletin board. The verification process requires voters to locate their ballots

using the tracker codes and verify the associated cryptographic proofs. However, usability studies have consistently shown that voter comprehension and utilization of verification procedures remains problematic [1].

The bulletin board architecture in Helios serves as the foundation for universal verifiability by providing a publicly accessible repository of all election data necessary for verification. The bulletin board contains encrypted ballots, cryptographic proofs, election parameters, and verification software. This transparency enables independent third parties to verify election integrity without requiring access to private system components or trusted election officials. Real-world deployments of Helios have provided valuable insights into the practical challenges of cryptographic voting systems. The system has been used successfully in numerous low-stakes elections, including university student government elections, professional association voting, and academic conference program committee selections. These deployments have demonstrated both the feasibility of end-to-end verifiable voting and the persistent challenges in achieving widespread voter participation in verification activities [3]. Performance analysis of Helios deployments has revealed scalability limitations that may impact its suitability for large-scale public elections. The computational overhead of homomorphic tallying grows linearly with the number of ballots and candidates, potentially creating performance bottlenecks in elections with hundreds of thousands of voters. Additionally, the bandwidth requirements for downloading and verifying election data may be prohibitive for voters with limited internet connectivity.

### 2.4.2 Estonian i-Voting System

Estonia's internet voting system represents the most successful large-scale implementation of remote digital voting in legally binding elections. Since 2005, Estonia has used internet voting for local, parliamentary, and European Parliament elections, with consistent growth in adoption rates among eligible voters [33]. The Estonian system leverages the country's comprehensive digital identity infrastructure, including mandatory identity cards equipped with PKI certificates. Voters authenticate using their identity cards and PIN codes, then cast ballots through a dedicated voting application. The system implements a unique "vote updating" feature that allows voters to change their vote multiple times, with only the final vote being counted. This approach is designed to mitigate coercion by enabling voters to cast coerced votes and later change them to their true preferences [23].

The cryptographic design of the Estonian system relies on standard public key encryption and digital signatures rather than the advanced cryptographic techniques used in systems like Helios. Ballots are encrypted using RSA encryption and signed with the voter's private key for authentication. The system uses a distributed trust model with multiple parties involved in key management and vote processing [31]. Extensive academic analysis of the Estonian system has revealed both strengths and vulnerabilities. The system's integration with national digital identity infrastructure provides strong voter authentication and has enabled high levels of public trust and adoption. However, security researchers have identified potential vulnerabilities in the system's client-side software and network communications [31]. The Estonian

experience provides valuable lessons about the political and social dimensions of digital voting adoption. Public acceptance of the system has grown consistently over time, with internet voting accounting for an increasing percentage of total votes cast in successive elections. This growth demonstrates that voters can become comfortable with digital voting technology when it is properly implemented and supported by appropriate infrastructure [33].

### 2.4.3 Scantegrity II

The Scantegrity voting system represents an innovative approach to combining paper-based voting with cryptographic verification. Developed by David Chaum and colleagues, Scantegrity enables end-to-end verification while maintaining the familiar interface of optical scan voting [12]. Scantegrity ballots appear similar to traditional optical scan ballots but include invisible ink that reveals confirmation codes when voters mark their choices. These confirmation codes serve as cryptographic receipts that voters can use to verify that their ballots were properly included in the election tally. The system provides individual verifiability without compromising ballot privacy or requiring voters to understand complex cryptographic concepts [10]. The system was deployed in the 2009 municipal election in Takoma Park, Maryland, representing the first use of end-to-end verifiable voting in a binding public election in the United States. Analysis of this deployment provided insights into the practical challenges of implementing cryptographic voting systems in real election environments [11].

### 2.4.4 Voatz Mobile Voting System

Voatz represents a commercial mobile voting platform that has been used in several pilot elections in the United States. The system targets overseas military voters and other absentee populations, utilizing smartphone technology to enable remote voting through a mobile application [30].

The Voatz system incorporates blockchain technology for ballot storage and verification, with the stated goal of providing transparency and auditability through distributed ledger mechanisms. Voters cast ballots through a mobile application that performs facial recognition and identity verification before enabling ballot marking and submission. However, comprehensive security analysis of the Voatz system has revealed significant vulnerabilities in multiple components of the platform. Researchers identified potential attack vectors including client-side vulnerabilities in the mobile application, insecure network communications, and weaknesses in the blockchain implementation. These findings have raised serious questions about the system's suitability for use in legally binding elections [30].

## 2.5 Security Requirements and Threat Models

Digital voting systems must address a complex landscape of security threats while maintaining the fundamental properties required for democratic elections. Understanding these threats and their mitigation strategies is essential for evaluating the security posture of different voting system implementations.

### 2.5.1 Threat Models

The threat model for digital voting systems encompasses a wide range of potential adversaries with varying capabilities and motivations. Nation-state actors represent the most sophisticated threat category, with the ability to conduct advanced persistent threats, compromise network infrastructure, and deploy sophisticated malware. These adversaries may seek to manipulate election results, undermine public confidence in electoral processes, or gather intelligence about voting patterns Criminal organizations may target voting systems for financial gain through vote buying schemes or ransom attacks against election infrastructure. Insider threats from election officials, system administrators, or vendor personnel represent another significant risk category, as these individuals may have privileged access to critical system components and data [25].

Hacktivist groups and politically motivated attackers may attempt to disrupt elections or manipulate results to advance specific ideological goals. These threats may involve website defacements, denial-of-service attacks, or attempts to compromise voting system integrity. The diversity of potential threats requires voting systems to implement comprehensive security measures that address both technical vulnerabilities and operational risks. Defense-in-depth strategies that layer multiple security controls are essential for protecting against sophisticated adversaries [34].

### 2.5.2 Attack Vectors

Digital voting systems face numerous potential attack vectors that adversaries may exploit to compromise election integrity or voter privacy. Client-side attacks represent a particularly significant threat for remote voting systems, as adversaries may compromise voter devices with malware that modifies vote choices or steals authentication credentials [31]. Network-based attacks can intercept or modify communications between voters and voting systems, potentially enabling ballot manipulation or voter impersonation. Man-in-the-middle attacks, DNS poisoning, and BGP hijacking represent specific network threats that voting systems must address through secure communication protocols and infrastructure hardening [34].

Server-side vulnerabilities in voting system software or infrastructure can provide adversaries with access to ballot databases, cryptographic keys, or system administration functions. Web application vulnerabilities, database injection attacks, and privilege escalation exploits represent common server-side attack vectors [21]. Supply chain attacks targeting voting system hardware or software development processes represent an emerging threat category that is difficult to detect and mitigate. These attacks may involve compromising development tools, inserting malicious code into system components, or modifying hardware during manufacturing processes.

### 2.5.3 Security Controls and Countermeasures

Effective security controls for digital voting systems must address the full spectrum of identified threats while maintaining system usability and performance. Cryptographic controls provide fundamental security properties including data confidentiality, integrity, and authentication. However, cryptographic implementations must

be carefully designed and validated to avoid common pitfalls such as weak key generation, improper algorithm usage, or side-channel vulnerabilities [5]

Access controls limit system access to authorized personnel and implement principle of least privilege to minimize the impact of potential compromises. Multi-factor authentication, role-based access controls, and privileged access management represent important access control mechanisms for voting systems. Audit and monitoring capabilities enable detection of security incidents and provide evidence for post-election audits. Comprehensive logging, real-time monitoring, and automated anomaly detection can help identify potential attacks or system anomalies [7].

## 2.6 Usability and Accessibility Considerations

The success of digital voting systems ultimately depends on their usability and accessibility for diverse voter populations. Usability challenges in voting systems can lead to voter disenfranchisement, increased error rates, and reduced public confidence in electoral processes.

### 2.6.1 Usability Challenges

Digital voting systems face unique usability challenges that differ significantly from traditional paper-based voting. The complexity of cryptographic verification procedures can overwhelm voters and reduce their willingness to participate in verification activities. Studies of end-to-end verifiable voting systems have shown that many voters either fail to understand verification procedures or choose not to perform verification checks [1]. The cognitive load imposed by digital voting interfaces can be particularly challenging for elderly voters or those with limited technological experience. Interface design decisions such as navigation methods, information presentation, and error handling can significantly impact voter success rates and satisfaction [18]. Mobile voting systems introduce additional usability challenges related to small screen sizes, touch interfaces, and variable network connectivity. These constraints require careful interface design to ensure that voters can successfully complete the voting process across diverse device types and network conditions [30].

### 2.6.2 Accessibility Requirements

Digital voting systems must comply with accessibility requirements to ensure equal access for voters with disabilities. The Americans with Disabilities Act and similar legislation in other jurisdictions mandate that voting systems provide equivalent functionality for voters with visual, auditory, motor, or cognitive impairments. Audio interfaces and screen reader compatibility are essential for voters with visual impairments, while alternative input methods may be required for voters with motor disabilities. The challenge lies in implementing these accessibility features without compromising ballot privacy or system security. Cognitive accessibility represents an often-overlooked aspect of voting system design. Clear language, simplified navigation, and error prevention can help voters with cognitive disabilities successfully complete the voting process. However, these design principles must be balanced

against the need to provide comprehensive election information and security features [6].

## 2.7 Challenges and Criticisms

Despite significant research and development efforts, digital voting systems continue to face substantial challenges and criticisms that limit their widespread adoption. These difficulties highlight that secure and trustworthy elections require more than just technical solutions; they also depend on social acceptance, political will, and institutional safeguards. Understanding these challenges is crucial for evaluating the current state of the field and identifying areas where further improvement is necessary.

### 2.7.1 Technical Challenges

The complexity of implementing secure digital voting systems presents some of the most pressing technical challenges. Modern elections are high-stakes targets, and even relatively small vulnerabilities can undermine confidence in the outcome. Software flaws in voting implementations have repeatedly been shown to expose systems to manipulation. High-profile audits of commercially deployed systems have revealed exploitable weaknesses, sometimes severe enough to allow an attacker to alter or discard ballots [34]. Such findings demonstrate that even systems designed with advanced cryptography are only as strong as their software engineering and deployment practices.

Scalability is another major technical concern. While systems like Helios perform reliably in small-scale elections, expanding to national contests with millions of voters introduces new stresses [2]. Performance bottlenecks, network congestion, and the computational demands of cryptographic protocols can all impact availability and degrade the voter experience during peak usage periods [2]. The challenge is not only to provide security guarantees but also to ensure that these guarantees hold under real-world conditions of heavy load and diverse infrastructures.

Key management further complicates secure deployment. In cryptographic voting systems, the secure generation, distribution, and storage of cryptographic keys is essential. If key material is mishandled or concentrated in a few trusted authorities, the entire election can be compromised. Designing robust key distribution frameworks that avoid single points of failure while still being manageable by election administrators remains an open problem [7].

### 2.7.2 Social and Political Challenges

Even when technical protections are strong, social and political factors can significantly affect the success or failure of digital voting initiatives. Public acceptance varies widely across different populations and political cultures. Concerns about privacy, security, and the potential for manipulation often lead to skepticism, regardless of the actual merits of specific systems [4]. Trust in elections is a deeply social phenomenon; if voters perceive a system as insecure, this perception alone can undermine legitimacy.

The digital divide presents another barrier. Reliable internet access, modern devices, and technological literacy cannot be assumed universally. Rural areas, older populations, or economically disadvantaged groups may be disproportionately excluded by digital-only solutions. Without careful design, digital voting risks reinforcing inequalities in participation by privileging those with better access to technology. Ensuring inclusivity therefore requires not only technical design but also policy support, voter education, and complementary mechanisms such as hybrid paper backups.

Political and legal frameworks also lag behind technological development. In many jurisdictions, the legal status of digitally cast ballots remains unclear. Disputes about recounts, challenges, or system failures may lack established procedures, creating uncertainty in contested elections [26]. Moreover, political resistance is not uncommon: some governments are reluctant to adopt internet voting due to fears of cyberattacks, public backlash, or international interference. Thus, adoption is shaped not only by what is technically possible but also by what is politically acceptable.

### 2.7.3 Verification and Audit Challenges

Verification and auditability are cornerstones of trustworthy elections, but their practical implementation poses challenges. End-to-end verifiable voting systems, such as Helios, provide strong theoretical guarantees that voters can confirm their ballots were "cast as intended, recorded as cast, and tallied as recorded [8]." Yet, in practice, voter participation in verification remains low. Studies show that many voters either do not understand verification procedures or are unwilling to perform them, reducing their effectiveness as safeguards [1].

Auditing also remains complex. Risk-limiting audits and post-election verification procedures rely on sophisticated statistical methods to provide assurance of election integrity. While powerful in theory, these methods are often difficult for election officials to implement correctly and even harder for the general public to interpret [32]. If audit procedures are too technical, they risk being perceived as opaque "black boxes," which undermines their ability to build public trust. Achieving both statistical rigor and public comprehensibility remains a critical challenge in this area.

### 2.7.4 Summary

Taken together, these challenges demonstrate that digital voting is still a developing field. Technical difficulties such as software security, scalability, and key management intersect with social and political barriers like trust, inequality, and legal uncertainty. Even verification and auditing, which are designed to inspire confidence, face real-world obstacles in adoption and usability. Addressing these criticisms requires a multidisciplinary approach that combines secure system design with careful attention to human factors, legal frameworks, and transparent governance. Until these issues are resolved, large-scale deployment of digital voting will remain controversial and contested.

## 2.8 Risk-Limiting Audits and Post-Election Verification

The development of risk-limiting audits represents a significant advancement in post-election verification procedures that bridges the gap between traditional election audits and the rigorous verification requirements of modern democratic systems. Risk-limiting audits provide statistical guarantees about election outcomes while maintaining practical feasibility for large-scale deployments.

### 2.8.1 Theoretical Foundations of Risk-Limiting Audits

The mathematical foundation of risk-limiting audits rests on statistical hypothesis testing principles adapted for electoral verification. The fundamental concept involves treating the reported election outcome as a null hypothesis that can be tested against physical evidence in the form of paper ballots. A risk-limiting audit with risk limit $\alpha$ provides assurance that if the reported outcome is incorrect, the probability of the audit failing to detect this error is at most $\alpha$ [32].

The SHANGRLA (Sets of Half-Average Nulls Generate Risk-Limiting Audits) framework developed by Stark provides a unified mathematical approach to conducting risk-limiting audits across diverse election types and voting systems. This framework generalizes traditional comparison audits to handle complex ballot structures, multiple contests, and various voting methods while maintaining rigorous statistical guarantees [32].

The statistical power of risk-limiting audits depends critically on the margin of victory in the audited contest. Contests with larger margins require smaller sample sizes to achieve the same risk limit, while close elections may require auditing a substantial portion of all ballots. This relationship between audit efficiency and election margins has important implications for audit planning and resource allocation.

### 2.8.2 Implementation Challenges in Risk-Limiting Audits

The practical implementation of risk-limiting audits faces several significant challenges that can impact their effectiveness and adoption. Ballot retrieval and organization systems must be designed to support efficient random sampling while maintaining chain of custody requirements. Many election jurisdictions lack the infrastructure necessary to quickly locate and retrieve randomly selected ballots from storage systems.

Human factors in audit implementation present another significant challenge. Audit procedures require careful training of election officials and observers to ensure accurate ballot interpretation and data recording. Discrepancies between audit team members in ballot interpretation can introduce errors that may compromise audit validity.

The integration of risk-limiting audits with existing election processes requires careful coordination between voting system vendors, election officials, and oversight bodies. Audit software must be compatible with diverse voting systems and election management databases while maintaining appropriate security controls and audit trails.

## 2.9 Ballot Marking Devices and Hybrid Systems

The emergence of ballot marking devices (BMDs) represents an attempt to combine the benefits of electronic voting interfaces with the auditability of paper-based systems. These hybrid systems generate voter-verified paper records while providing electronic assistance for ballot completion.

### 2.9.1 Design Principles and Implementation Approaches

Ballot marking devices typically present electronic interfaces that allow voters to make their selections using touchscreens, audio interfaces, or other input methods. Once voting is complete, the device prints a paper ballot that serves as the official record of the voter's choices. This paper ballot can be reviewed by the voter before submission and serves as the basis for recounts and audits.

The design of BMD interfaces must balance usability requirements with the need to produce accurate paper records. Interface design decisions regarding information presentation, navigation methods, and confirmation procedures can significantly impact both voter satisfaction and the accuracy of the resulting paper ballots.

### 2.9.2 Security Considerations for Ballot Marking Devices

The security model for ballot marking devices must address threats to both the electronic interface and the paper record generation process. Malicious software running on BMDs could potentially modify vote selections between voter input and paper ballot printing, creating a gap between voter intent and the recorded vote.

Research by Bernhard et al. has demonstrated that voters often fail to carefully review the paper ballots produced by BMDs, potentially missing modifications made by malicious software. This finding raises important questions about the effectiveness of voter verification in hybrid systems and the assumptions underlying their security models [9].

The verification burden placed on voters in BMD systems requires careful consideration of cognitive load and verification procedures. Effective verification requires voters to carefully compare their intended votes with the printed ballot, but studies suggest that many voters either skip this step or perform it inadequately.

## 2.10 Mobile and Remote Voting Systems

The proliferation of mobile devices and ubiquitous internet connectivity has driven interest in mobile voting solutions that could potentially increase voter participation and reduce election administration costs. However, mobile voting systems face unique security and usability challenges that distinguish them from traditional polling place voting.

### 2.10.1 Technical Architecture of Mobile Voting Systems

Mobile voting systems typically operate through dedicated applications installed on voter devices or through web-based interfaces accessible via mobile browsers.

These systems must implement authentication mechanisms to verify voter eligibility, provide secure ballot marking interfaces, and transmit completed ballots to election servers.

The client-side security model for mobile voting presents fundamental challenges that are difficult to address through cryptographic means alone. Mobile devices are general-purpose computing platforms that may be compromised by malware, subject to various attack vectors, and controlled by users who may not understand security implications of their actions.

### 2.10.2 Blockchain Integration in Mobile Voting

Several mobile voting implementations have incorporated blockchain technology with the stated goal of providing transparency and auditability through distributed ledger mechanisms. The Voatz system represents one of the most prominent examples of blockchain-based mobile voting used in real elections.

However, comprehensive security analysis of blockchain-based voting systems has revealed that the use of blockchain technology does not address the fundamental security challenges inherent in remote voting systems. The security properties of the blockchain are only as strong as the systems that feed data into the ledger, and compromised client devices can submit fraudulent data regardless of the blockchain's integrity properties [30].

The complexity of blockchain implementations in voting systems may actually increase the attack surface available to adversaries while providing limited security benefits. The distributed nature of blockchain systems can make security analysis more difficult and may introduce new categories of vulnerabilities related to consensus mechanisms and network protocols.

## 2.11 International Perspectives and Comparative Analysis

The global landscape of digital voting adoption varies significantly across different political systems, regulatory environments, and technological infrastructures. Examining international experiences provides valuable insights into the factors that influence successful digital voting deployment.

### 2.11.1 European Approaches to Digital Voting

European countries have pursued diverse approaches to digital voting, reflecting different priorities regarding security, usability, and public acceptance. The Estonian i-Voting system represents the most comprehensive implementation of remote digital voting in binding elections, while other European countries have focused on polling place electronic voting or pilot programs with limited scope.

The European Union's regulatory framework for digital voting emphasizes the importance of maintaining traditional democratic principles while leveraging technological innovations. The Council of Europe's recommendations on electronic voting provide guidelines for member states considering digital voting implementation, though these recommendations are not legally binding.

Switzerland's approach to digital voting has involved extensive pilot programs and gradual expansion of electronic voting options. The Swiss system incorporates multiple cryptographic verification mechanisms and has been subject to public security reviews. However, political opposition and security concerns have led to temporary suspensions of the program.

### 2.11.2 Developing Country Implementations

Several developing countries have implemented digital voting systems as part of broader efforts to modernize electoral processes and reduce election administration costs. These implementations often face different challenges related to infrastructure limitations, technical capacity, and resource constraints.

Brazil's electronic voting system represents one of the largest deployments of electronic voting technology globally, with over 100 million voters using electronic voting machines in national elections. The Brazilian system uses custom hardware and software designed specifically for voting applications, with strong physical security controls and centralized vote counting procedures.

India's Electronic Voting Machines (EVMs) represent another large-scale implementation that has been used in national and state elections for over two decades. The Indian system emphasizes simplicity and reliability, using custom hardware with minimal software complexity to reduce potential failure modes and security vulnerabilities.

## 2.12 Human Factors and Voter Behaviour

Understanding how voters interact with digital voting systems is crucial for designing systems that support accurate vote capture and maintain public confidence in electoral processes. Human factors research in voting systems encompasses usability, accessibility, and cognitive aspects of voter behaviour.

### 2.12.1 Cognitive Load and Decision Making in Digital Voting

Digital voting interfaces can impose significant cognitive load on voters, particularly when they incorporate complex verification procedures or present information in unfamiliar formats. The cognitive demands of understanding cryptographic verification procedures may exceed the capabilities or motivation of many voters, potentially reducing the effectiveness of end-to-end verification systems.

Research on voter decision-making processes has revealed that voters often use cognitive shortcuts and heuristics when completing ballots, particularly in elections with many contests or candidates. Digital voting interface design can either support or hinder these natural decision-making processes depending on how information is presented and organized.

The timing and pacing of voting decisions can be significantly affected by digital interfaces. Unlike paper ballots that allow voters to review their complete set of choices before submission, many digital voting systems present contests sequentially,

potentially making it difficult for voters to reconsider earlier decisions or understand the relationships between different contests.

### 2.12.2 Trust and Acceptance Factors

Public trust in digital voting systems depends on multiple factors including perceived security, ease of use, and confidence in election administration. Research has shown that trust in voting technology is influenced by both technical factors and social/political context, with significant variation across different demographic groups and political affiliations.

The transparency of digital voting systems plays a crucial role in building public trust, but transparency must be balanced against security requirements and operational considerations. Open-source voting systems may provide greater transparency but require sophisticated technical knowledge to evaluate, potentially limiting their effectiveness in building broad public confidence.

Media coverage and public discourse about digital voting can significantly influence public acceptance, with security incidents or technical failures receiving disproportionate attention compared to successful deployments. This dynamic creates challenges for election officials seeking to build public support for digital voting initiatives.

## 2.13 Future Directions and Emerging Technologies

The evolution of digital voting systems continues to be driven by advances in cryptography, changes in voter expectations, and new threat landscapes. Understanding emerging trends and technologies is essential for anticipating future developments in the field.

### 2.13.1 Post-Quantum Cryptography Implications

The potential development of large-scale quantum computers poses long-term threats to the cryptographic foundations of current digital voting systems. Most public-key cryptographic systems used in voting, including those based on discrete logarithms and integer factorization, would be vulnerable to quantum attacks using Shor's algorithm.

The transition to post-quantum cryptographic algorithms will require careful evaluation of their suitability for voting applications. Post-quantum algorithms typically have different performance characteristics and security assumptions compared to current cryptographic systems, potentially requiring significant changes to voting system architectures.

The timeline for quantum computing threats remains uncertain, but the lengthy development and deployment cycles for voting systems require early consideration of post-quantum cryptographic requirements. Election systems deployed today may need to remain secure for decades, potentially spanning the transition to quantum-resistant cryptography.

### 2.13.2 Artificial Intelligence and Machine Learning Applications

Artificial intelligence and machine learning technologies offer potential applications in voting systems, including automated ballot processing, anomaly detection, and voter assistance. However, the use of AI in voting systems raises important questions about transparency, accountability, and potential bias.

Machine learning algorithms could potentially improve the accuracy of optical character recognition in ballot scanning systems, enabling more reliable processing of hand-marked ballots. However, the black-box nature of many machine learning systems may conflict with the transparency requirements for voting systems.

AI-powered voter assistance systems could help voters navigate complex ballots or provide information about candidates and issues. However, the potential for bias in AI systems raises concerns about fairness and equal treatment of all voters.

### 2.13.3 Integration with Digital Identity Systems

The increasing adoption of digital identity systems in various countries creates opportunities for tighter integration between identity verification and voting systems. Digital identity credentials could potentially simplify voter authentication while maintaining privacy and security requirements.

However, the integration of voting systems with digital identity infrastructure also creates new potential points of failure and attack vectors. Compromises of digital identity systems could have cascading effects on voting system security and public confidence in electoral processes.

The centralization of identity verification functions may conflict with the distributed trust models preferred for voting systems. Balancing the benefits of integrated identity systems with the need for resilient and trustworthy voting processes remains an ongoing challenge.

## 2.14 Regulatory and Legal Framework Evolution

The legal and regulatory landscape for digital voting continues to evolve as jurisdictions gain experience with different technologies and approaches. Understanding these regulatory trends is important for anticipating future requirements and constraints on digital voting systems.

### 2.14.1 Certification and Standards Development

The development of comprehensive standards for digital voting systems requires coordination between technical experts, election officials, and legal authorities. Existing standards such as the Voluntary Voting System Guidelines in the United States provide frameworks for evaluating voting system security and functionality, but these standards continue to evolve as technology advances.

International standardization efforts face challenges related to different legal systems, electoral procedures, and technical requirements across jurisdictions. However, common security principles and best practices can provide a foundation for

harmonized approaches to digital voting system evaluation.

The certification process for voting systems must balance thoroughness with practical considerations including cost, time requirements, and the need for ongoing security updates. Traditional certification approaches may not be well-suited to software-intensive systems that require frequent updates to address emerging threats.

### 2.14.2 Privacy and Data Protection Considerations

The application of data protection regulations such as the European Union's General Data Protection Regulation (GDPR) to voting systems creates new requirements for privacy protection and data handling. These regulations may conflict with traditional approaches to election record keeping and audit procedures.

The concept of data minimization in privacy regulations may support the use of cryptographic techniques that limit the collection and retention of personal information in voting systems. However, audit and recount requirements may necessitate the retention of detailed records that could potentially identify individual voters.

Cross-border data flows in internet voting systems may be subject to data localization requirements that limit the jurisdictions where election data can be processed or stored. These requirements could significantly impact the architecture and deployment options for digital voting systems.

## 2.15 Summary

The literature reveals a field marked by significant theoretical progress alongside persistent practical challenges. Cryptographic techniques for ensuring privacy, integrity, and verifiability in digital voting systems are well-established, yet their implementation in real-world settings continues to face technical, social, and political obstacles. The gap between cryptographic guarantees and practical usability remains a fundamental challenge that requires ongoing research and development.

The diversity of approaches adopted by systems such as Helios, Estonian i-Voting, and Voatz illustrates the range of strategies used to balance security, usability, and deployment requirements [2]. Each system reflects distinct trade-offs and assumptions shaped by its electoral context, offering valuable insights into the complexity of digital voting implementation.

Digital voting system research and implementation remain multifaceted and rapidly evolving, driven by technological advances, shifting security requirements, and increasing experience with real-world deployments. While notable progress has been made in addressing theoretical concerns, practical challenges—such as usability, scalability, and public acceptance—continue to hinder widespread adoption. Addressing these technical and socio-political challenges is essential for realizing the full potential of digital voting while preserving the integrity and trustworthiness of democratic processes. These considerations form the foundation for the detailed analysis of selected systems presented in the following chapters.

# 3 Theoretical Framework

## 3.1 Introduction

This chapter presents the theoretical framework used to analyse and compare digital voting systems. It outlines the key security properties, threat models, and evaluation criteria that form the basis for the case studies in later chapters. Drawing on established research in voting security, cryptographic protocol analysis, and human–computer interaction, the framework provides a structured and comprehensive approach to assessing different system designs.

Digital voting systems must satisfy a unique set of election-specific security requirements while remaining usable, scalable, and practical for real-world deployment. These demands often create tensions—for example, strong security and privacy mechanisms may reduce usability or introduce operational challenges. The framework developed here acknowledges these trade-offs and offers a clear method for identifying the strengths and limitations of each voting system. It also supports systematic comparison across systems that may rely on different cryptographic techniques and architectural models.

### 3.1.1 Privacy and Ballot Secrecy

Privacy in digital voting systems encompasses multiple related but distinct requirements. Ballot secrecy, the fundamental principle that individual vote choices must remain confidential, represents the most basic privacy requirement. This property ensures that voters cannot be subject to retaliation, coercion, or discrimination based on their voting choices. In digital systems, ballot secrecy must be maintained not only during the voting process but throughout the entire election lifecycle, including vote storage, transmission, and tallying phases. The implementation of ballot secrecy in digital voting systems typically relies on cryptographic techniques such as encryption and anonymization protocols. However, the effectiveness of these techniques depends heavily on proper implementation and the absence of side-channel information leakage. Unlike paper-based systems where ballot secrecy is achieved through physical processes and procedural controls, digital systems must rely on mathematical guarantees that may be vulnerable to implementation errors or unforeseen attack vectors.

Forward privacy represents an additional consideration in digital voting systems, ensuring that ballot secrecy is maintained even if cryptographic keys or system components are compromised after the election. This property requires careful key management and may necessitate the use of cryptographic techniques such as forward-secure encryption or secure deletion protocols. The anonymity of voters represents another dimension of privacy that extends beyond ballot secrecy. While ballot secrecy ensures that vote choices remain confidential, voter anonymity requires that the act of voting itself cannot be linked to specific individuals. This distinction becomes particularly important in systems that maintain audit trails or verification mechanisms that could potentially be used to identify voters who participated in verification activities.

### 3.1.2 Integrity and Authenticity

Integrity guarantees in digital voting systems ensure that votes cannot be altered, deleted, or fabricated without detection. This property encompasses both the integrity of individual ballots and the integrity of the overall election process, including vote collection, transmission, storage, and tallying operations. Ballot integrity requires mechanisms to detect any unauthorized modification of individual vote records. This is typically achieved through cryptographic techniques such as digital signatures or message authentication codes that provide mathematical proof of ballot authenticity. However, the effectiveness of these mechanisms depends on secure key management and the proper implementation of cryptographic protocols. System integrity encompasses the broader requirement that all components of the voting system operate correctly and have not been compromised or manipulated. This includes the integrity of software components, hardware platforms, network communications, and operational procedures. Achieving system integrity requires comprehensive security controls including secure software development practices, hardware security measures, and robust operational security procedures.

The temporal aspect of integrity presents unique challenges in digital voting systems. Unlike paper ballots that provide inherent evidence of tampering through physical alterations, digital records can be modified without leaving obvious traces unless specific protections are implemented. This requires the use of tamper-evident logging systems, cryptographic timestamps, and other mechanisms to provide evidence of the integrity of election data over time. Election integrity extends beyond technical measures to include procedural and organizational controls that ensure the proper conduct of elections. This encompasses voter authentication procedures, ballot access controls, result verification processes, and dispute resolution mechanisms. The integration of technical and procedural integrity measures is essential for maintaining public confidence in digital voting systems.

### 3.1.3 Verifiability

Verifiability represents one of the most significant theoretical advances in digital voting research, enabling mathematical verification of election correctness without requiring trust in voting system software or administrators. End-to-end verifiability encompasses several distinct but related properties that together provide comprehensive assurance of election integrity. Cast-as-intended verifiability enables voters to confirm that their ballots accurately reflect their intended vote choices and have been properly submitted to the voting system [8, 28]. This property addresses the risk that malicious software or hardware could modify vote choices without the voter's knowledge. Implementation typically involves providing voters with cryptographic receipts or confirmation codes that can be verified against publicly posted election data.

Recorded-as-cast verifiability ensures that ballots submitted by voters are accurately recorded in the election database without modification or deletion. This property protects against attacks that might alter or remove ballots after they have been cast. Cryptographic techniques such as digital signatures and append-only data structures are typically used to provide recorded-as-cast verification. Tallied-

as-recorded verifiability enables verification that the published election results accurately reflect the ballots recorded in the system. This property ensures that the tallying process has been performed correctly and that no votes have been miscounted or omitted from the final results. Homomorphic encryption and zero-knowledge proofs are commonly used to enable tallying verification while maintaining ballot privacy.

Individual verifiability allows voters to personally verify that their specific ballots were included in the election tally without revealing their vote choices. This is typically implemented through receipt-based systems where voters receive cryptographic receipts that can be checked against publicly posted ballot lists or verification data. Universal verifiability enables any party, including independent observers and auditors, to verify the correctness of the overall election result using publicly available information. This property ensures that election verification does not depend on the cooperation of voters or election officials and can be performed by independent third parties.

The implementation of verifiability properties often involves complex trade-offs with other system requirements. Verification procedures must be designed to be comprehensible to ordinary voters while maintaining cryptographic rigor. The usability of verification mechanisms significantly impacts their effectiveness, as verification procedures that are too complex or time-consuming may be ignored by voters.

### 3.1.4 Coercion Resistance

Coercion resistance represents one of the most challenging security properties to achieve in digital voting systems, particularly those that enable remote voting [24]. This property requires that voters cannot be coerced or bribed to vote in particular ways, even if coercers can observe the voting process or demand proof of vote choices. Traditional polling place voting provides natural coercion resistance through the secret ballot environment and the practical difficulty of monitoring voter behavior within polling booths [24]. Remote digital voting systems eliminate many of these physical protections and must rely on technical measures to prevent coercion.

Receipt-freeness, a related property, requires that voters cannot generate convincing proof of their vote choices even if they wish to cooperate with coercers. This property helps prevent vote buying by eliminating the ability of voters to demonstrate their compliance with payment demands. However, implementing receipt-freeness while maintaining verifiability properties presents significant technical challenges. The "voting booth" assumption that underlies many coercion resistance analyses may not hold for remote voting systems where voters may be subject to direct observation during the voting process [24]. Some systems attempt to address this through mechanisms such as "panic passwords" or the ability to cast multiple votes with only the final vote being counted, but these approaches have limitations and may not provide adequate protection in all coercion scenarios.

Everlasting privacy represents an extreme form of coercion resistance that requires ballot secrecy to be maintained even against adversaries with unlimited computational resources and access to all system components and data [24]. This property

may be necessary in high-stakes elections where the revelation of vote choices could have severe consequences for voters.

## 3.2 Framework for Evaluation

The evaluation framework developed for this research provides a systematic approach for analyzing digital voting systems across multiple dimensions while maintaining focus on the fundamental requirements of democratic elections. This framework enables consistent evaluation of systems that may employ different architectural approaches and technical solutions.

### 3.2.1 Security Analysis Criteria

The security analysis component of the framework examines the cryptographic protocols and security mechanisms employed by each voting system. This analysis evaluates the theoretical security properties provided by the system design as well as the practical security guarantees achievable in real-world deployments. Cryptographic protocol analysis examines the mathematical foundations of the security mechanisms employed by each system. This includes evaluation of encryption schemes, digital signature algorithms, zero-knowledge proof systems, and other cryptographic primitives used to achieve security properties. The analysis considers both the theoretical security of the underlying cryptographic techniques and their proper implementation within the voting system context.

Threat model coverage assesses how effectively each system addresses the range of potential adversaries and attack scenarios relevant to digital voting. This evaluation considers the assumptions made by system designers about adversary capabilities and motivations, and analyzes whether these assumptions are realistic for the intended deployment environments. Implementation security examines the practical security characteristics of system implementations, including software security practices, vulnerability management, and operational security controls. This analysis recognizes that theoretical cryptographic guarantees may be undermined by implementation vulnerabilities or operational failures.

Security assumption analysis evaluates the trust assumptions underlying each system's security model. This includes assumptions about the honesty of system administrators, the security of cryptographic key management, the integrity of software and hardware components, and the behaviour of voters and election officials.

### 3.2.2 Usability Assessment Framework

The usability assessment framework evaluates the human factors aspects of digital voting systems, recognizing that usability limitations can undermine both security and democratic participation. This assessment considers the diverse needs of voter populations and the practical constraints of election environments. Voter interface evaluation examines the design and functionality of voter-facing interfaces, including ballot marking procedures, verification mechanisms, and error handling. This analysis considers factors such as cognitive load, navigation complexity, information presentation, and accessibility for voters with disabilities.

Verification usability assessment analyzes the comprehensibility and practicality of cryptographic verification procedures. This evaluation recognizes that verification mechanisms that are too complex or time-consuming may be ignored by voters, undermining the security benefits they are intended to provide. Administrative usability examines the interfaces and procedures used by election officials and system administrators. This includes setup and configuration procedures, election monitoring capabilities, result processing workflows, and incident response mechanisms.

Accessibility analysis evaluates compliance with accessibility requirements and the accommodation of diverse voter needs. This assessment considers factors such as language support, assistive technology compatibility, and accommodation of voters with various types of impairments. Learning curve assessment examines the training and support requirements for both voters and election officials. This analysis considers the complexity of system operation and the resources required to achieve competent system use.

### 3.2.3 Practical Deployment Analysis

The practical deployment analysis examines the real-world feasibility and operational characteristics of digital voting systems. This analysis recognizes that systems that perform well in laboratory environments may face significant challenges when deployed in actual election contexts. Infrastructure requirements analysis evaluates the technical infrastructure, organizational capabilities, and regulatory frameworks necessary for successful system deployment. This includes assessment of network infrastructure, hardware requirements, software dependencies, and integration with existing election systems.

Scalability assessment examines system performance under realistic load conditions and analyzes the ability to support large-scale elections with millions of voters. This evaluation considers factors such as computational requirements, network bandwidth utilization, and database performance under peak loads. Operational complexity analysis examines the administrative burden and operational procedures required for system deployment and management. This includes consideration of staff training requirements, procedural complexity, and the integration of digital voting systems with existing election administration processes.

Cost-benefit analysis evaluates the economic aspects of system deployment, including initial implementation costs, ongoing operational expenses, and potential cost savings compared to traditional voting methods. This analysis considers both direct costs and indirect factors such as increased accessibility and potential efficiency gains. Risk assessment examines the potential failure modes and their consequences for electoral integrity and public confidence. This analysis considers both technical risks such as system failures or security breaches and operational risks such as procedural errors or inadequate staff training.

## 3.3 Threat Models

The threat modeling framework for digital voting systems must account for the unique characteristics of electoral environments and the diverse range of potential

adversaries who might seek to compromise election integrity or voter privacy. This section establishes comprehensive threat models that inform the security analysis of the selected voting systems.

### 3.3.1 Adversary Classification

The classification of potential adversaries provides a structured approach for analyzing the security requirements and defensive measures necessary for digital voting systems. Different adversary types possess varying capabilities, motivations, and access levels that influence their potential impact on election security. Nation-state adversaries represent the most sophisticated and well-resourced threat category. These adversaries may possess advanced persistent threat capabilities, access to zero-day exploits, and the ability to compromise network infrastructure or supply chains. Their motivations may include influencing election outcomes, gathering intelligence about political processes, or undermining public confidence in democratic institutions. Nation-state adversaries may conduct long-term campaigns involving multiple attack vectors and sophisticated operational security measures.

The capabilities of nation-state adversaries include advanced malware development, network infrastructure compromise, supply chain infiltration, and social engineering operations. These adversaries may also have access to insider personnel within government agencies, technology companies, or election administration organizations. Defending against nation-state adversaries requires comprehensive security measures and may necessitate assumptions about the limits of their capabilities. Criminal organizations may target voting systems for financial gain through vote buying schemes, extortion attacks, or fraud operations. These adversaries typically possess moderate technical capabilities and may focus on attacks that provide direct monetary returns. Criminal organizations may also be hired by other parties to conduct election-related attacks, providing plausible deniability for the actual sponsors.

Hacktivist groups and politically motivated attackers may seek to disrupt elections, manipulate results, or demonstrate vulnerabilities in electoral systems. These adversaries often possess moderate technical skills and may be motivated by ideological goals rather than financial gain. Their activities may include website defacements, denial-of-service attacks, or publication of system vulnerabilities. Insider threats encompass individuals with privileged access to voting system components, including election officials, system administrators, software developers, and vendor personnel. Insider adversaries may have legitimate access to critical system components and may be able to conduct attacks that would be difficult or impossible for external adversaries. Insider threats may be motivated by financial gain, political ideology, or coercion by external parties.

Individual attackers or small groups may attempt to manipulate elections through various means, including voter impersonation, ballot stuffing, or system compromise. While these adversaries typically possess limited technical capabilities compared to nation-states or organized criminal groups, they may still pose significant threats to smaller-scale elections or specific election components.

### 3.3.2 Attack Scenarios

The development of realistic attack scenarios provides concrete examples of how different adversaries might attempt to compromise digital voting systems. These scenarios inform security requirements and help evaluate the effectiveness of defensive measures. Client-side compromise scenarios involve adversaries gaining control of voter devices through malware infections, compromised software, or physical access attacks. In these scenarios, adversaries may modify vote choices without voter knowledge, steal authentication credentials, or monitor voter behavior for coercion purposes. Client-side attacks are particularly relevant for remote voting systems where voters use personal devices that may have varying levels of security protection.

Malware-based attacks represent a significant threat category for digital voting systems, particularly those that rely on software running on voter devices. Advanced malware may be capable of modifying ballot selections, intercepting authentication credentials, or providing false feedback to voters about their vote choices. The sophistication of modern malware and its ability to evade detection systems creates significant challenges for client-side security in voting applications. Network-based attack scenarios involve adversaries intercepting or manipulating communications between voters and voting systems. These attacks may include man-in-the-middle attacks that alter ballot submissions, DNS poisoning that redirects voters to malicious websites, or network surveillance that compromises voter privacy. Network attacks may be conducted by adversaries with access to network infrastructure or through the compromise of network equipment.

BGP hijacking and other network infrastructure attacks represent sophisticated threat scenarios where adversaries manipulate internet routing to intercept or redirect voting system traffic. These attacks require significant technical capabilities and may be conducted by nation-state adversaries or other well-resourced attackers with access to network infrastructure. Server-side compromise scenarios involve adversaries gaining unauthorized access to voting system servers or databases. Successful server-side attacks may enable adversaries to modify election results, access voter information, or disrupt election operations. These attacks may be conducted through exploitation of software vulnerabilities, social engineering, or physical access to server infrastructure.

Database manipulation attacks represent a critical threat scenario where adversaries modify stored ballot data or election results. These attacks may be difficult to detect if proper audit mechanisms are not in place and could have severe consequences for election integrity. Database security measures including access controls, encryption, and audit logging are essential for preventing and detecting these attacks. Supply chain compromise scenarios involve adversaries inserting malicious code or hardware into voting system components during the development or manufacturing process. These attacks may be extremely difficult to detect and could provide persistent access to voting systems. Supply chain security requires comprehensive vendor vetting, code auditing, and hardware verification procedures.

Social engineering attacks target human elements of voting systems, including voters, election officials, and technical personnel. These attacks may involve phishing

campaigns to steal authentication credentials, impersonation of technical support personnel, or manipulation of procedural controls. Social engineering attacks often serve as initial vectors for more sophisticated technical attacks.

### 3.3.3 Attack Impact Assessment

The assessment of potential attack impacts provides a framework for understanding the consequences of successful compromises and prioritizing defensive measures. Different types of attacks may have varying impacts on election integrity, voter privacy, and public confidence in electoral processes. Vote manipulation attacks that successfully alter individual ballots or election results represent the most severe impact category. These attacks directly compromise the fundamental purpose of elections and may alter the outcome of political contests. The impact of vote manipulation depends on the scale of the attack and the margin of victory in affected contests.

Large-scale vote manipulation that alters election outcomes represents a catastrophic failure scenario that could undermine democratic governance and public confidence in electoral institutions. Even unsuccessful attempts at large-scale manipulation may have significant impacts on public trust and political stability. Privacy violations that reveal individual vote choices may have severe consequences for affected voters, including retaliation, discrimination, or violence. The impact of privacy breaches may extend beyond the immediate election to affect future political participation and democratic engagement.

System availability attacks that disrupt voting operations may prevent eligible voters from casting ballots, potentially affecting election outcomes and disenfranchising voters. The impact of availability attacks depends on their duration, scope, and the availability of alternative voting methods. Denial-of-service attacks against voting systems may be particularly impactful during peak voting periods or in jurisdictions with limited voting infrastructure. These attacks may create long delays that discourage voter participation or prevent some voters from casting ballots before polling deadlines.

Information disclosure attacks that reveal sensitive election administration information may compromise operational security and provide intelligence for future attacks. While these attacks may not directly alter election outcomes, they may facilitate more serious attacks or undermine confidence in election security. Coercion and vote buying facilitated by system vulnerabilities may compromise the freedom and secrecy of ballot choices. The impact of these attacks may be difficult to measure directly but could have significant effects on democratic participation and representation.

## 3.4 Evaluation Methodology

The evaluation methodology provides a systematic approach for applying the theoretical framework to the analysis of selected digital voting systems. This methodology ensures consistent evaluation across different systems while accounting for their unique characteristics and design approaches.

### 3.4.1 Analytical Approach

The analytical approach combines qualitative assessment with structured comparison to provide comprehensive understanding of system capabilities and limitations. This approach recognizes that digital voting systems involve complex interactions between technical, social, and operational factors that cannot be fully captured through purely quantitative measures. Multi-dimensional analysis examines each system across the security, usability, and practical deployment dimensions established in the evaluation framework. This approach ensures that the analysis considers all relevant aspects of system performance and does not overemphasize any single dimension at the expense of others.

Comparative case study methodology enables systematic comparison of different systems while acknowledging their unique characteristics and design contexts. This approach facilitates identification of common patterns, trade-offs, and best practices across different voting system implementations. Evidence-based assessment relies on published research, security audits, deployment reports, and other documented evidence to support analytical conclusions. This approach ensures that the evaluation is grounded in empirical data rather than theoretical speculation or vendor claims.

### 3.4.2 Data Sources and Evidence

The evaluation relies on multiple categories of evidence to ensure comprehensive and balanced analysis. Primary sources include peer-reviewed academic publications, security research papers, and official documentation from system developers and deploying organizations. Security audit reports provide critical evidence about system vulnerabilities, implementation quality, and real-world security posture. These reports often reveal practical security issues that may not be apparent from theoretical analysis or system documentation alone.

Deployment case studies and post-election reports provide insights into the practical challenges and operational characteristics of voting systems in real-world election environments. These sources help identify the gap between theoretical capabilities and practical performance. Usability studies and user experience research provide evidence about the human factors aspects of voting systems and their impact on voter behavior and election outcomes. This evidence is particularly important for assessing the practical viability of complex verification procedures.

### 3.4.3 Analytical Limitations

The evaluation methodology acknowledges several important limitations that affect the scope and conclusions of the analysis. These limitations are inherent in the available evidence and the practical constraints of academic research. The analysis relies primarily on publicly available information and published research rather than independent security testing or experimental evaluation. This limitation means that the evaluation cannot identify previously unknown vulnerabilities or conduct original empirical research on system performance.

The dynamic nature of cybersecurity threats and the ongoing evolution of voting system technologies means that security assessments may become outdated as new

vulnerabilities are discovered or systems are updated. The evaluation attempts to address this limitation by focusing on fundamental design characteristics rather than specific implementation details. The limited deployment experience with some systems, particularly newer technologies like blockchain-based voting, constrains the availability of real-world performance data and lessons learned. This limitation requires careful interpretation of theoretical claims and vendor assertions.

The complexity of voting system security makes it difficult to provide definitive assessments of overall system security posture. The evaluation attempts to address this by clearly identifying assumptions, limitations, and areas of uncertainty in the analysis.

## 3.5 Summary

The theoretical framework established in this chapter provides the analytical foundation for evaluating and comparing digital voting systems across multiple critical dimensions. The framework encompasses security properties essential for democratic elections, practical considerations relevant to real-world deployment, and usability factors that determine voter acceptance and effective system operation. The security properties framework identifies privacy, integrity, verifiability, and coercion resistance as fundamental requirements that digital voting systems must satisfy [24]. Each property presents unique implementation challenges and potential conflicts with other system requirements. The framework provides structured approaches for analyzing how different systems address these requirements and the trade-offs involved in their design decisions.

The evaluation methodology combines qualitative assessment with comparative analysis to provide comprehensive understanding of system capabilities and limitations. This approach recognizes the multi-dimensional nature of voting system evaluation and the need to consider technical, social, and operational factors simultaneously. The threat modeling framework provides systematic approaches for analyzing the security risks facing digital voting systems and evaluating the adequacy of defensive measures. The framework considers diverse adversary types and attack scenarios while acknowledging the unique characteristics of electoral environments.

The practical deployment analysis framework addresses the real-world feasibility and operational characteristics that determine whether digital voting systems can be successfully implemented in actual election contexts. This analysis recognizes that systems that perform well in laboratory environments may face significant challenges when deployed at scale in actual elections. This theoretical framework guides the detailed case study analysis presented in subsequent chapters and enables systematic comparison of the selected voting systems. The framework's multi-dimensional approach ensures that the evaluation considers all relevant aspects of system performance while maintaining focus on the fundamental requirements of democratic elections.

# 4 Methodology

## 4.1 Introduction

This chapter outlines the methodology employed to analyze and compare three digital voting systems: Helios, Estonian i-Voting, and Voatz. The study adopts a qualitative comparative case study approach, which enables an in-depth examination of each system while also facilitating meaningful cross-case comparisons. This methodology provides a structured framework to explore how variations in design and implementation affect security, usability, and deployment feasibility, ultimately generating insights to guide future digital voting initiatives.

The study combines a thorough literature review with technical analysis and structured comparative evaluation, ensuring that both theoretical and practical perspectives are considered. Given that digital voting systems are socio-technical in nature, involving interactions between technology, user experience, and operational constraints, a qualitative approach is particularly appropriate. The study is designed to balance technical rigor with practical relevance, ensuring that findings are evidence-based and analytically robust.

## 4.2 Research Design

The research follows a qualitative comparative case study methodology, which is well-suited for analysing complex systems in real-world contexts. Case studies allow for detailed examination of systems, taking into account interactions between technology, legal frameworks, administrative procedures, and social factors. The comparative dimension highlights patterns, trade-offs, and best practices, offering insights into how different design choices affect system performance. Because digital voting systems involve both technical and human factors, the analysis relies on structured frameworks alongside careful judgment informed by empirical evidence.

The evaluation of each system is guided by three main dimensions: security, usability, and deployment feasibility. Security is assessed through an examination of cryptographic protocols, threat resistance, integrity, verifiability, and coercion resistance. Usability focuses on voter accessibility, interface design, error prevention, and administrative ease of use, while deployment feasibility considers scalability, infrastructure requirements, and practical implementation challenges. This multidimensional framework ensures a comprehensive assessment, allowing each system to be evaluated fairly across all relevant aspects.

To maintain an evidence-driven approach, the study relies primarily on peer-reviewed research, independent audits, deployment reports, and documented user experiences rather than vendor claims. This ensures that conclusions are grounded in verifiable data and reflect both theoretical principles and practical realities.

## 4.3 Systems Selected for Analysis

The three systems selected for analysis—Helios, Estonian i-Voting, and Voatz—were chosen to represent a diversity of technical approaches, real-world deployments, and

documented research. Helios is an open-source, academically developed voting system that uses homomorphic encryption, allowing privacy-preserving tallying and wide deployment in organizational elections [2]. It serves as a key reference in verifiable voting research. The Estonian i-Voting system, in operation since 2005, integrates with the country's digital ID infrastructure and includes mechanisms such as vote updating to reduce coercion risks. Its long-standing national deployment provides a model for large-scale internet voting. Voatz, a commercial platform, employs blockchain technology and biometric authentication to enable mobile voting. Although it has faced security criticism, Voatz illustrates emerging trends in mobile and distributed ledger-based voting.

The selected systems provide both technical diversity and contextual variation. They operate in different environments, ranging from small organizational elections to national elections, and they are supported by sufficient documentation for analysis. By comparing systems with varied designs, operational contexts, and technical foundations, the study captures a broad perspective on the challenges and opportunities in digital voting.

## 4.4 Evaluation Criteria

Each system is evaluated across the dimensions of security, usability, and deployment readiness. Security is considered in terms of privacy, vote integrity, verifiability, and resistance to coercion, focusing on encryption techniques, key management, procedural safeguards, and mechanisms for individual and universal verification. Usability is assessed through voter accessibility, interface clarity, support for multiple languages, cognitive load, error prevention, and administrative usability, including system configuration, monitoring, and documentation. Deployment readiness considers scalability, computational and network requirements, resilience under peak loads, and the feasibility of integrating the system into existing electoral infrastructure. This structured approach ensures that comparisons are systematic, transparent, and grounded in evidence.

## 4.5 Limitations and Constraints

The study faces several limitations. Reliance on published sources constrains the discovery of previously unknown vulnerabilities, and rapid technological evolution means that findings may become outdated. Proprietary restrictions, particularly for commercial systems such as Voatz, limit access to detailed technical information. Legal, political, and policy factors fall outside the scope of this analysis.

Analytical constraints include the complexity of interactions between software, hardware, protocols, and procedures, which makes comprehensive security evaluation challenging. Limited deployment data for newer systems constrains long-term reliability and scalability assessment, while usability evaluation inherently involves subjective judgment despite the use of structured frameworks. Additionally, results may not generalize to all electoral contexts. Despite these limitations, the methodology provides a framework for evaluating digital voting systems, offering valuable insights into their strengths, weaknesses, and suitability for democratic elections.

# 5 Case Studies

## 5.1 Helios Voting System

Helios represents an academically driven approach to verifiable digital voting and is widely cited in research as a reference implementation of end-to-end verifiable elections [2]. It is an open-source platform designed primarily for educational, union, and small-scale organizational elections, where transparency and verifiability are valued above scalability. Its architecture relies heavily on exponential ElGamal encryption, which enables ballots to be cast and tallied securely while preserving voter privacy. Each vote is encrypted individually, and thanks to the homomorphic properties of ElGamal, the system can compute the election outcome without decrypting individual ballots. This provides a mathematical guarantee of both integrity and privacy.

In practice, Helios has been used by universities, non-profit organizations, and professional societies [2]. For instance, it has facilitated student government elections in Europe and North America, as well as leadership elections within international academic associations. These real-world applications demonstrate its practicality in controlled settings where participants are technologically literate and where the electorate size is relatively small. A major strength of Helios is its open-source nature, which allows independent experts to review, test, and audit the system code [2]. This openness strengthens trust by ensuring that vulnerabilities can be identified publicly rather than hidden.

Despite its academic success, Helios faces several challenges in real-world elections [2]. Its dependence on the voter's device and browser introduces risks: if the client machine is compromised by malware, the ballot may be altered before encryption, undermining the system's guarantees. Furthermore, Helios has limited scalability, as it was not designed for national elections involving millions of voters [2]. Its performance requirements, combined with limited usability features, make it impractical for high-stakes, large-scale contexts. Ultimately, Helios demonstrates the feasibility of end-to-end verifiable systems but highlights the trade-off between academic rigor and operational scalability [2].

## 5.2 Estonian i-Voting System

Estonia's i-Voting system stands as the longest-running and most mature example of nationwide digital voting. Since its introduction in 2005, it has been used in parliamentary, municipal, and European Parliament elections, with adoption steadily increasing over time. In the 2019 parliamentary elections, over 44% of votes were cast online, showing strong public trust and widespread acceptance. The system is tightly integrated with Estonia's digital identity infrastructure, relying on Public Key Infrastructure (PKI) and cryptographic smart cards for strong voter authentication. Each voter receives a government-issued ID card with embedded chips that enable secure digital signatures, providing both privacy and verifiability [16].

A unique feature of the Estonian model is the ability for voters to recast their ballots multiple times during the voting period. Only the final vote is counted,

which reduces the risk of coercion by allowing voters to override any pressured choices. This feature, combined with extensive audits and transparency measures, has helped Estonia address criticisms while reinforcing public trust.

However, criticisms remain. Security researchers have raised concerns about reliance on trusted hardware and government infrastructure, which could become single points of failure. The system's resilience against large-scale cyberattacks has also been debated, particularly given the geopolitical tensions in the Baltic region. Furthermore, while Estonia's digital identity system is highly developed, it is unclear whether the same approach could be transplanted to larger and more diverse democracies where digital identity adoption is fragmented or contested.

Overall, Estonia's i-Voting provides valuable insights into what is possible when digital voting is integrated into a comprehensive national digital ecosystem. It highlights both the opportunities for large-scale deployment and the challenges of maintaining transparency and security over time.

## 5.3 Voatz Voting System

Voatz represents a commercial, mobile-first approach to digital voting, designed with accessibility and convenience in mind. The system leverages blockchain technology for auditability and uses biometric authentication (such as fingerprint or facial recognition) to verify voter identity. It has been piloted in U.S. elections for overseas military personnel and citizens with disabilities, including trials in West Virginia (2018), Utah, and Denver. These pilots were framed as experiments in expanding participation to populations that face barriers in traditional voting.

The use of blockchain is central to Voatz's model. By recording ballots in a distributed ledger, the system provides tamper-evidence and immutability, reducing reliance on a single trusted authority. In principle, this creates a transparent audit trail that voters and election officials can verify. In addition, its smartphone-based interface makes it easier for remote voters to participate without specialized hardware.

Despite its innovative approach, Voatz has faced significant criticism from security researchers. Independent audits, including a 2020 analysis by MIT, uncovered vulnerabilities that could allow attackers to alter votes or compromise ballot secrecy. Other concerns include the risks of client-side malware on voters' smartphones and the potential for network-based attacks. Additionally, because Voatz is a proprietary commercial system, its source code is not fully open to the public, limiting independent verification and contributing to skepticism among experts.

Voatz illustrates both the promise and the pitfalls of mobile-based voting. On the one hand, it demonstrates how new technologies can lower barriers to participation. On the other hand, it underscores that accessibility and convenience must not come at the expense of security and transparency. Until its vulnerabilities are resolved and its processes made more open, Voatz remains an experimental system rather than a proven solution for large-scale, high-stakes elections.

# 6 Comparative Analysis

When comparing Helios, Estonian i-Voting, and Voatz, several patterns emerge in their cryptographic foundations, security properties, and real-world deployment.

Helios is often viewed as a benchmark in academic discussions of digital voting. It uses homomorphic encryption and provides strong theoretical guarantees of privacy and tally integrity. Its open-source nature also promotes transparency and independent verification. However, Helios is limited in practice: it was not designed for large-scale national elections and remains vulnerable to client-side threats, such as malware on a voter's device.

Estonian i-Voting represents the most mature example of digital voting in national elections. By combining Public Key Infrastructure (PKI) with smart card authentication, Estonia has achieved both privacy and verifiability at scale. The system has been refined through repeated nationwide use since 2005, showing that careful integration with existing national identity infrastructure can overcome many practical barriers. At the same time, critics have questioned its reliance on trusted hardware and its vulnerability to coercion, reminding us that large-scale deployment does not mean immunity from criticism.

Voatz reflects a different direction, focusing on mobile accessibility and blockchain-backed auditability. Its emphasis on smartphones makes it attractive for increasing participation among remote or marginalized voters. Yet, security audits and independent reports have revealed vulnerabilities in client devices and communication networks. Moreover, its proprietary nature restricts external validation, making it difficult to establish public trust in its claims.

Across all three systems, common strengths can be identified. Each makes use of advanced cryptographic safeguards and incorporates some form of voter verification. However, persistent weaknesses remain. Client-side vulnerabilities are a recurring challenge, as even the most secure cryptography cannot protect against compromised devices. Coercion resistance is another unsolved issue, especially in remote or unsupervised voting settings. Usability also poses difficulties, particularly for voters with limited digital literacy or access to secure devices.

Scalability emerges as a key differentiator. Helios is well suited for small-scale elections, such as in universities or professional associations, but is not practical for national contests. Estonia has demonstrated that large-scale internet voting is possible, though not without controversy. Voatz, while innovative, has yet to prove its robustness in high-stakes, nationwide settings.

Taken together, these comparisons suggest that no single system currently provides a complete solution. Trade-offs are unavoidable between security, usability, and accessibility. The challenge for future systems is to strike a more effective balance across these dimensions. Progress will likely require innovations in coercion resistance, stronger protections for mobile voting, and architectures capable of scaling without undermining trust.

To support policymakers and developers, visual comparisons can be especially helpful. Tables summarizing cryptographic techniques, security properties, and practical implementation challenges would make contrasts clearer and highlight crit-

ical lessons. Such tools can translate complex technical findings into insights that are more accessible to decision-makers and the general public.

# 7 Discussion

The case studies examined in this thesis highlight both the opportunities and the challenges of adopting digital voting systems. On the one hand, digital platforms can significantly improve accessibility and efficiency, particularly for overseas citizens, individuals with disabilities, or those in remote areas. By reducing physical and logistical barriers, digital systems have the potential to broaden participation and strengthen democratic engagement. On the other hand, the transition from traditional paper-based methods is far from straightforward. Security risks, uneven levels of digital literacy, and the fragility of public trust continue to shape the debate. Even systems that have been tested and refined over time such as Estonia's i-Voting remain under scrutiny, demonstrating that no system is immune to criticism or vulnerability.

A recurring theme across the systems studied is the importance of trust and transparency. For citizens to accept digital elections, systems must not only be secure in theory but must also appear trustworthy and verifiable in practice. Voters must feel confident that their ballots are private, correctly counted, and free from manipulation. Inclusivity is equally important: systems should ensure participation across diverse groups, including those with disabilities, varying language needs, and limited technical familiarity. If these concerns are not addressed, digital voting could unintentionally widen the gap between those who are digitally literate and those who are not, reinforcing social and political inequalities.

Looking forward, several research and innovation directions stand out. The integration of post quantum cryptography is critical for future-proofing digital elections against emerging computational threats. Usability improvements through intuitive interface design, public education campaigns, and comprehensive voter training will play a key role in making digital voting more accessible and trusted. At the same time, hybrid approaches that combine traditional methods with digital solutions may provide resilience and flexibility. For example, systems that allow digital vote casting but also generate auditable paper trails could offer both efficiency and security, bridging the gap between innovation and reliability.

There are also broader ethical and societal considerations. The expansion of digital voting raises questions about the digital divide, the role of private companies in public elections, and the long-term implications of relying on technologies that may outpace regulation. Governments, technologists, and civil society must work together to ensure that the adoption of digital voting strengthens democratic values rather than undermining them. This means approaching digital elections not just as technical systems, but as social institutions that require ongoing scrutiny, transparency, and public dialogue.

In conclusion, the findings of this thesis emphasize that digital voting cannot succeed through technology alone. Strong cryptography and secure protocols are essential, but they must be embedded within systems that are socially inclusive, ethically responsible, and operationally realistic. The experiences of Helios, Estonian i-Voting, and Voatz demonstrate both the progress that has been made and the challenges that remain. Ultimately, building a trustworthy digital voting sys-

tem requires balancing innovation with caution, and technical strength with social legitimacy.

Digital voting is not a destination but a process a gradual evolution shaped by technology, society, and politics. Its future will depend not only on solving cryptographic puzzles but also on fostering trust, inclusivity, and resilience. By learning from past experiments and present systems, democracies can take careful, informed steps toward a future where digital voting complements, rather than replaces, the fundamental principles of free and fair elections.

# References


[1] Claudia Z. Acemyan et al. "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II". In: *USENIX Journal of Election Technology and Systems (JETS)* 2.3 (2014), pp. 26–56. URL: https://www.usenix.org/journal/jets/issues/0203.

[2] Ben Adida. "Helios: Web-based Open-Audit Voting." In: *USENIX security symposium*. Vol. 17. 2008, pp. 335–348. URL: https://www.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf.

[3] Ben Adida et al. "Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios". In: *EVT/WOTE* 9.10 (2009), p. 10. URL: http://usenix.org/events/evtwote09/tech/full_papers/adida-helios.pdf.

[4] R Michael Alvarez and Thad E Hall. *"Electronic elections: The perils and promises of digital democracy"*. Princeton University Press, 2010.

[5] Ross J Anderson. *"Security engineering: a guide to building dependable distributed systems"*. John Wiley & Sons, 2010.

[6] Benjamin B Bederson et al. "Electronic voting system usability issues". In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2003, pp. 145–152. DOI: 10.1145/642611.642638.

[7] Susan Bell et al. "STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System". In: *2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13)*. 2013. DOI: 10.48550/arXiv.1211.1904.

[8] Josh Benaloh. "Simple Verifiable Elections." In: *EVT* 6 (2006), pp. 5–5. URL: https://www.usenix.org/legacy/event/evt06/tech/full_papers/benaloh/benaloh.pdf?ref=https://githubhelp.com.

[9] Matthew Bernhard et al. "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" In: *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2020, pp. 679–694. DOI: 10.1109/SP40000.2020.00118.

[10] Richard Carback et al. "Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy". In: *19th USENIX Security Symposium (USENIX Security 10)*. 2010. URL: https://www.usenix.org/event/sec10/tech/full_papers/Carback.pdf.

[11] David Chaum et al. "Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes". In: *IEEE transactions on information forensics and security* 4.4 (2009), pp. 611–627. DOI: 10.1109/TIFS.2009.2034919.

[12] David Chaum et al. "Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting". In: *IEEE Security & Privacy* 6.3 (2008), pp. 40–46. DOI: 10.1109/MSP.2008.70.

[13] David L Chaum. "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms". In: *Communications of the ACM* 24.2 (1981), pp. 84–90. DOI: 10.1007/978-1-4615-0239-5_14.

[14] Margaret Chen et al. "Better Ballots". In: (2008). URL: https://www.policyarchive.org/handle/10207/8289.

[15] Véronique Cortier et al. "Election Verifiability for Helios under Weaker Trust Assumptions". In: *Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19*. Springer. 2014, pp. 327–344. DOI: 10.1007/978-3-319-11212-1_19.

[16] Piret Ehin et al. "Internet voting in Estonia 2005–2019: Evidence from eleven elections". In: *Government Information Quarterly* 39.4 (2022), p. 101718. DOI: 10.1016/j.giq.2022.101718.

[17] Taher ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". In: *IEEE transactions on information theory* 31.4 (1985), pp. 469–472. DOI: 10.1109/TIT.1985.1057074.

[18] Sarah P Everett et al. "Electronic voting machines versus traditional methods: Improved preference, similar performance". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 2008, pp. 883–892. DOI: 10.1145/1357054.1357195.

[19] Jun Furukawa and Kazue Sako. "An Efficient Scheme for Proving a Shuffle". In: *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings 21*. Springer. 2001, pp. 368–387. DOI: 10.1007/3-540-44647-8_22.

[20] Shafi Goldwasser, Silvio Micali, and Chales Rackoff. "The knowledge complexity of interactive proof-systems". In: *Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali*. 2019, pp. 203–225. DOI: 10.1145/3335741.3335750.

[21] Rop Gonggrijp and Willem-Jan Hengeveld. "Studying the Nedap/Groenendaal ES3B voting computer: a computer security perspective". In: *Proceedings of the USENIX workshop on accurate electronic voting technology*. 2007, pp. 1–1. URL: https://dl.acm.org/doi/abs/10.5555/1323111.1323112.

[22] Mogens Herman Hansen. *"The Athenian democracy in the age of Demosthenes: structure, principles, and ideology"*. University of Oklahoma Press, 1999.

[23] Sven Heiberg, Peeter Laud, and Jan Willemson. "The Application of I-Voting for Estonian Parliamentary Elections of 2011". In: *International Conference on E-Voting and Identity*. Springer. 2011, pp. 208–223. DOI: 10.1007/978-3-642-32747-6_13.

[24] Ari Juels, Dario Catalano, and Markus Jakobsson. "Coercion-resistant electronic elections". In: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. 2005, pp. 61–70. DOI: 10.1145/1102199.1102213.

[25] Donald P Moynihan. "Building Secure Elections: E-Voting, Security, and Systems Theory". In: *Public administration review* 64.5 (2004), pp. 515–528. DOI: 10.1111/j.1540-6210.2004.00400.x.

[26] Pippa Norris. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. 2003. DOI: 10.22230/cjc.2003v28n1a1352.

[27] Pascal Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *International conference on the theory and applications of*

*cryptographic techniques*. Springer. 1999, pp. 223–238. DOI: 10.1007/3-540-48910-X_16.

[28] Ronald L Rivest. "On the notion of 'software independence'in voting systems". In: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 366.1881 (2008), pp. 3759–3767. DOI: 10.1098/rsta.2008.0149.

[29] Adi Shamir. "How to share a secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613. DOI: 10.1145/359168.359176.

[30] Michael A Specter, James Koppel, and Daniel Weitzner. "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections". In: *29th USENIX Security Symposium (USENIX Security 20)*. 2020, pp. 1535–1553. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/specter.

[31] Drew Springall et al. "Security Analysis of theEstonian Internet Voting System". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, pp. 703–715. DOI: 10.1145/2660267.2660315.

[32] Philip B Stark. "Sets of Half-Average Nulls Generate Risk-Limiting Audits: SHANGRLA". In: *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24*. Springer. 2020, pp. 319–336. DOI: 10.1007/978-3-030-54455-3_23.

[33] Kristjan Vassil et al. "The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015". In: *Government information quarterly* 33.3 (2016), pp. 453–459. DOI: 10.1016/j.giq.2016.06.007.

[34] Scott Wolchok et al. "Attacking the Washington, D.C. Internet Voting System". In: *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers 16*. Springer. 2012, pp. 114–128. DOI: 10.1007/978-3-642-32946-3_10.