Data Privacy in Internet Voting Systems

A Comparative Research on Internet Voting in Estonia, Switzerland, France, and Norway

Alara Zeybek
Computer Science
Bilkent University
Ankara, TURKEY
alara.zeybek@ug.bilkent.edu.tr

GROUP 10

Aytekin İsmail
Computer Science
Bilkent University
Ankara, TURKEY
aytekin.ismail@ug.bilkent.edu.tr

İpek Sönmez
Computer Science
Bilkent University
Ankara, TURKEY
ipek.sonmez@ug.bilkent.edu.tr

Berkay Gündüz
Computer Science
Bilkent University
Ankara, TURKEY
berkay.gunduz@ug.bilkent.edu.tr

Sıla Özel
Computer Science
Bilkent University
Ankara, TURKEY
sila.ozel@ug.bilkent.edu.tr

ABSTRACT

Voting is an important part of democracy when done correctly. Since the early-2000s, internet voting has been introduced to improve and simplify the voting process. However, this method involves sensitive personal data that must be stored and transmitted securely. This study compares the Internet voting systems in Estonia, Switzerland, France, and Norway. We examine voter participation, computational cost, voter anonymity, system availability, resilience and transparency. The research uses a mixed-method approach with a literature review, and threat assessments for each system, and findings are presented in graphs and tables.

KEYWORDS

Vote verifiability, voter authentication, voter authorization, anonymity, unlinkability, transparency, and voter turnout.

1 Introduction

Electronic voting (e-voting) refers to using electronic devices in the voting process. This includes voting kiosks, ballot scanners, e-Pen solutions, and remote internet voting systems [1]. Our study focuses only on internet voting (i-voting) systems implemented in Estonia, Switzerland, France, and Norway. While each country's system has been studied individually, there is limited research comparing these systems in terms of voter turnout, computing requirements, voter privacy, system availability and transparency. We propose a privacy framework based on voter participation, computational cost, voter anonymity, system availability, resilience and transparency. The different features of each country's i-voting system make this comparative analysis valuable for assessing and improving these systems.

Ideally, internet voting systems should increase voter participation and make vote verification, voter authentication, and authorization easier. However, real implementations have faced significant challenges. Estonia pioneered i-voting in 2005 and continues using it today, with about 51% of votes in the 2023 elections coming through this system [2]. Despite this success, the system wasn't perfect from the start. Security experts identified vulnerabilities and published technical reports recommending improvements [3].

Meanwhile, Switzerland began testing online voting systems in 2000 in three regions. The government prioritized security over speed, leading to more secure systems. They also developed a thorough certification framework that allowed different regions to use different online voting systems. This approach distinguishes the Swiss system from those in Norway, Estonia, and France, where governments typically select a single vendor through a public bidding process [4].

In France, the government tried online voting during the COVID-19 pandemic due to physical restrictions. They used Neovote's online voting system. Research conducted at Bordeaux University in 2022 revealed security weaknesses, some related to data privacy. For example, the password recovery process was vulnerable to interception attacks, and the registration process relied on "private" information that was actually shared with colleagues [5].

Norway tested an i-voting system in 2011. The voting process was straightforward and included vote verification using a 4-digit code sent by text message to build public trust. However, this verification system had an unexpected outcome: as more voters verified their votes, more instances of vote manipulation were discovered. Still, verification was an important step toward greater transparency [6]. Unlike some test programs, Norway stopped its i-voting experiments in 2014 due to limited political support, deciding further testing was unnecessary [7].

Overall, i-voting systems in these countries have various strengths and weaknesses. Some achieve higher voter turnout but experience data breaches. Others may be technically sound and private but see limited use due to low demand, as in Norway's case.

In the following sections, we discuss the features and challenges of these i-voting systems. We examine the threat models, assess and compare the systems using our criteria, and propose a privacy framework for more systematic evaluation. We conclude by suggesting directions for future research.

2 Internet Voting Systems

Internet voting systems allow eligible voters to cast ballots remotely using the public Internet. To be trustworthy, they must authenticate and authorize each voter (e.g. via e-ID cards or one-time SMS codes), protect voter privacy through unlinkability (using cryptographic envelopes or mixnets), ensure data integrity and end-to-end verifiability (with return codes or receipts), and remain available and resilient under failures or attacks through distributed servers and redundancy [1].

2.1 Privacy Enhancing Techniques

Key cryptographic tools for preserving voter privacy include blind signatures (to get ballots signed without revealing their content), mixnets (to shuffle and re-encrypt votes), homomorphic encryption (to tally votes in encrypted form), and zero-knowledge proofs (to prove a ballot's validity without disclosing the vote). Together, these techniques keep ballots secret while allowing voters and auditors to verify correct counting [2].

2.1.1 Blind Signatures

Blind signature schemes allow a voter to obtain a signature on their (encrypted) ballot from an eligibility authority without revealing its contents. Concretely, the voter "blinds" their ballot before sending it for signing; the authority signs the blinded message, and the voter then "unblinds" it to obtain a valid signature on the original ballot. This guarantees that only eligible voters can produce validly signed ballots, yet the authority cannot link any signature back to a particular voter. [8]

2.1.2 Mixnets

Mix networks (mixnets) break the link between incoming and outgoing messages by shuffling and re-encrypting batches of ciphertexts across multiple servers. In an Internet voting context, encrypted ballots are sent through a cascade of mix servers; each server re-encrypts and permutes the batch, ensuring that the final output cannot be linked to the original sender. This provides strong unlinkability and unobservability for cast votes. [8]

2.1.3 Homomorphic Tallying

Homomorphic encryption enables the election authority to compute the overall tally directly on encrypted ballots, without first decrypting individual votes. Voters encrypt their choices under a homomorphic scheme (e.g., Paillier or BGN); the authority multiplies (or adds) all ciphertexts to obtain an encryption of the sum. Only once the aggregate is formed is a single decryption performed, revealing the final result while preserving each vote's confidentiality. [8]

2.1.4 Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKPs) allow a voter (prover) to convince the election authority (verifier) that their encrypted ballot is well-formed (e.g., encodes a valid choice) without revealing any information about the choice itself. In many protocols, voters attach a ZKP that their ciphertext lies in the allowed message space; the authority checks this proof before including the ballot in the tally. Such proofs underpin anonymous credential systems (e.g., Idemix) and ensure correctness without sacrificing anonymity. [8]

2.2 Threat Model

Our threat model for i-voting systems integrates explicit components and clear definitions to thoroughly analyze threats, vulnerabilities, and potential harms concerning data privacy. The model includes four primary components: Voter, Internet Device, Vote Storage, and Monitor.

- **Voter:** Participants that enter credentials and cast votes.
- **Internet Device:** Hardware or software utilized by voters to encrypt and transmit votes.
- **Vote Storage:** System responsible for securely storing encrypted votes.
- **Monitor:** Entity responsible for observing and ensuring the integrity of the voting process.

Threat actors considered in our model include:

1. **Attacker with Forged Identity:** Capable of impersonating voters, voting multiple times, unauthorized access to administrative functionalities, vote manipulation, and voter anonymity breaches.
2. **Attacker with Access to Vote Storage:** Capable of unauthorized data manipulation, accessing sensitive stored data,

modifying vote outcomes, breaching voter anonymity, and tampering with audit logs.

3. Attacker with Auxiliary Information about Voters: Potential to exploit additional information to compromise voter anonymity and data privacy.

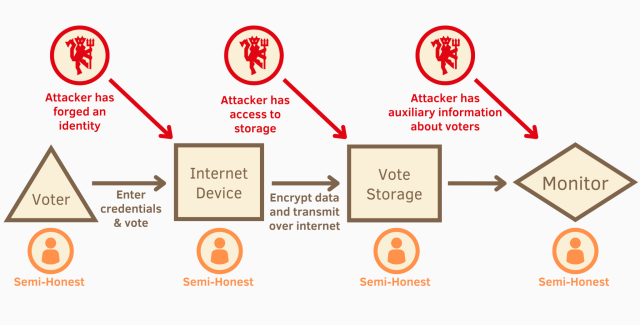

Fig. 1. *Overview of the i-voting system threat model. The attacker is modeled with three primary capabilities: forging identities to impersonate voters, accessing storage to modify or leak data, and using auxiliary information to infer private voter details. All system components are modeled as semi-honest.*

Our threat model presupposes a semi-honest stance for all system components, indicating general compliance with established protocols but acknowledging potential passive vulnerabilities. Each identified threat will be analyzed by evaluating specific vulnerabilities and clearly defining associated harms, such as compromised voter anonymity or altered election outcomes. This structured approach facilitates a precise assessment of privacy risks, enabling targeted mitigations tailored to maintain the robustness and integrity of the evaluated i-voting systems.

3 Methodology

The aim of this report is to conduct comparative research on the i-voting systems in Estonia, Switzerland, France, and Norway. The research process for this report can be categorized into three following groups:

Examination of documentation: Studying relevant documentation related to the i-voting system published by the national election committees, including guidelines, and specifications. This includes both the selected countries' reports and OSCE reports on elections.

Literature Review: Analyzing previous research on internet voting systems, the history of the internet voting systems and known vulnerabilities, and improvement suggestions from cybersecurity researchers.

Proposal of a privacy framework: Proposing a privacy framework based on the criteria of voter participation, transparency of the voting protocol, anonymity, computational cost, and availability and resilience of voting systems.

The novelty we introduce is a detailed analysis of these four countries' i-voting systems from a privacy-preserving perspective.

4 Research Scope

We focus on Estonia, Switzerland, France, and Norway because together they span the full spectrum of i‑voting approaches: Estonia is the world's first and only nationwide system with consistently high online uptake [2], Switzerland's cautious, canton-based trials under a rigorous open-source and certification regime [9], France's rapid "pandemic" deployment of a closed-source vendor solution with limited adoption [5], and Norway's small-scale pilots featuring SMS-based receipts that were ultimately discontinued [10]. By comparing these four cases, we capture varied governance models, technical architectures, and levels of voter engagement.

Our analysis covers each country's implementation history, legal framework, user authentication methods, privacy techniques, and real-world usage statistics. We examine why these particular systems were chosen, ranging from boosting turnout among expatriates (Switzerland, Norway) to emergency-only use (France) to full democratic integration (Estonia), and how their differing goals and constraints shaped design trade-offs in privacy, verifiability, and resilience.

4.1 French I-Voting System

The Neovote platform, used extensively in French e-voting, is presented as a highly secure platform in line with the strictest standards imposed by CNIL and ANSSI. According to this framework, systems like Neovote that claim to operate at the highest security level (level 3) must ensure ballot box transparency for all voters, enable transparency verification through third-party tools, and guarantee that vote counting can be verified after the election [5, 9].

4.1.1 Transparency and Obfuscation Practices

A critical issue raised in the audit of the Neovote system is its lack of transparency. Although it is presented as fully in-house developed and compliant with end-to-end verifiability standards, Neovote is a closed-source platform whose code is extremely obfuscated. Public access to the source code, documentation, developer information, and cryptographic architecture is mostly nonexistent, preventing meaningful third-party audits [5]. This is contrary to Kerckhoff's principle, which is the basis of cryptographic good practice and states that security within a system should not depend on secrecy of the system design [5]. Also, techniques such as blocking the Wayback Machine and manual inclusion of outdated cryptographic components further

obstruct transparency and deviate from ANSSI's guidance to use well-maintained, industry-standard libraries [5]. Additionally, the client-side JavaScript code examined appears to be deliberately obfuscated, with variable and function names seemingly randomized with each request, complicating independent security analysis [5].

4.1.2. Cryptographic Aspects and Used Libraries.

Even though Neovote is closed-source and does not publicly provide access to its code, researchers were still able to analyze the system by examining client-side JavaScript from the browser and performing reverse engineering on those web components (and APKs in other cases). In the end, the analysis revealed that Neovote integrates components from the outdated and unmaintained asmcrypto.js library [5]. This third-party cryptographic library was manually copied into the system's codebase, including unmerged pull requests, thereby violating secure development practices [5]. The library itself has not been updated since 2018 and includes cryptographic primitives that are no longer considered secure [5]. The library was optimized for performance rather than security and cannot be considered a standard industry solution.

Similar cryptographic misuses were observed in the 2021 French consular election [9]. The official APK client used improperly implemented AES-GCM encryption, lacked message authentication tags, and generated cryptographic keys through insecure randomness sources [9]. The absence of key derivation functions and proper key agreement protocols further compromised vote integrity [9].

4.1.3 Verification and Vote Integrity

Studies underscore the systemic failure to implement end-to-end verifiability [5, 9]. In Neovote's system, votes are not cryptographically linked to the receipts issued to voters, which undermines any voter-initiated verification [5]. Instead, results are handed off to election organizers for publication, opening the door to potential manipulation [5]. The receipt system is inherently flawed, caught in a trilemma: if receipts can be used to prove votes, voter secrecy is lost; if not, the system can suppress votes without detection; and if attackers gain access to receipts, voter anonymity can be compromised [5].

Technical issues further weaken the system. The vote verification tool is unreliable in large-scale elections, making it susceptible to denial-of-service (DoS) attacks [5]. Ballot boxes lack cryptographic signatures, enabling adversaries to create counterfeit ballot boxes [5]. Worse, the hash construction method allows the creation of fake receipts that are indistinguishable from legitimate ones [5].

4.1.4. Exploitable Design in Real-World Deployments

The French consular election APK, reverse-engineered by researchers, exposed the fragile nature of the client application [9]. The APK was downloaded at the time of voting, making it vulnerable to man-in-the-middle (MITM) attacks and supply chain compromises [9]. Furthermore, the confirmation mechanism—intended to reassure voters—was not cryptographically bound to the actual vote, enabling attackers to spoof confirmations [9]. Demonstrated attack scenarios included ballot stuffing using compromised credentials, malicious client applications discarding or altering votes, and fake confirmations misleading users into thinking their votes were cast successfully [9].

4.2 Norwegian I-Voting System

The Norwegian i-voting system was first introduced as a trial during the municipal elections of 2011 and later used in the parliamentary elections of 2013. Developed by Scytl, a Spanish company specializing in electronic voting solutions, the primary focus of the Norwegian i-voting system is ensuring robust data privacy alongside election integrity and voter anonymity [10][11].

4.2.1 Data Privacy Techniques

The Norwegian i-voting system utilizes sophisticated cryptographic techniques to ensure data privacy throughout the voting process. Primarily, the system employs ElGamal encryption, which leverages homomorphic properties, enabling encrypted votes to be re-encrypted and blinded without compromising privacy. This cryptographic method ensures that individual voter choices remain concealed at all stages, from submission to counting [12].

Another critical data privacy technique involves the use of zero-knowledge proofs. These proofs allow voters and authorities to validate the correctness of vote encryption, re-encryption, and eventual decryption without revealing any sensitive information. Such cryptographic proofs ensure that the integrity and authenticity of ballots can be verified without exposing the content of individual votes, thus preserving voter privacy [12].

Moreover, the system distributes cryptographic keys among multiple authorities (the Ballot Box (BB), Receipt Generator (RG), and Decryption Service (DS)), following a threshold cryptography scheme. No single authority possesses the complete key required for decrypting votes, significantly mitigating risks associated with key compromise or internal collusion. This separation of cryptographic powers is a cornerstone of the system's privacy guarantees [12].

4.2.2 Receipt and Verification Mechanism

A distinctive feature of the Norwegian system designed to protect voter privacy is the generation and use of voter receipts. These

receipts are sent to voters through an out-of-band channel (typically SMS), allowing voters to verify their submitted votes independently. Receipt codes are precomputed and distributed securely before elections via a postal service, adding a layer of trust and reducing reliance on digital communications. By using distinct channels for receipt code delivery and vote casting, the system minimizes the risk that compromised digital channels can lead to voter privacy breaches [13].

4.2.3 Vulnerabilities and Privacy Concerns

Despite these robust privacy techniques, potential vulnerabilities have been identified. Notably, the security and privacy of the Norwegian i-voting system depend critically on the assumption that the Ballot Box (BB) and Receipt Generator (RG) do not collude. [13] highlighted that if BB and RG cooperate, they could reconstruct the private key held by the Decryption Service (DS), thus compromising voter privacy. To counteract this vulnerability, it is suggested that stronger separation and additional cryptographic measures should be implemented to prevent collusion scenarios explicitly [13].

Additionally, the reliance on external communication channels (postal and SMS services) for transmitting voter receipts introduces a potential privacy risk if these channels are compromised or intercepted. To enhance the robustness of these channels, incorporating cryptographic integrity checks or employing additional secure communication layers is recommended [13].

4.2.4 Formal Verification of Privacy

The privacy protections of the Norwegian system have been subjected to rigorous formal analyses using applied pi-calculus methodologies. [12] provided comprehensive proofs verifying ballot secrecy under several corruption scenarios, including those involving compromised voters and certain compromised authorities. These formal analyses provide high confidence in the system's ability to protect voter privacy under realistic threat scenarios, reaffirming the robustness of its cryptographic foundations [12].

Gjøsteen's analysis further validates the security assumptions underpinning the Norwegian system, focusing explicitly on the cryptographic primitives and their ability to maintain data privacy. His work emphasizes the novel cryptographic techniques used for return code generation, which are crucial for ensuring voter privacy and preventing vote tampering [10].

In conclusion, the Norwegian i-voting system implements advanced cryptographic mechanisms and privacy-focused techniques to ensure robust data protection throughout the election process. While it remains resilient under formal analyses, continuous improvements, particularly addressing vulnerabilities related to internal collusion and external communication channels, are necessary for maintaining high levels of voter trust and privacy.

4.3 Switzerland I-Voting System

Switzerland began experimenting with i-voting in 2003, when the Canton of Geneva conducted the country's first online ballot as a pilot project [14]. In subsequent years, more cantons joined trials, primarily to facilitate voting for Swiss citizens living abroad and to counteract declining turnout [15]. Unlike Estonia's centralized system, the Swiss approach has been decentralized: individual cantons deploy i-voting systems on a trial basis under federal oversight. Two primary systems emerged: Geneva's open-source CHVote [16] platform and Swiss Post's sVote system, based on technology from Scytl.

By the mid-2010s, 14 cantons had conducted binding online voting trials, mainly for expatriates, accumulating over 300 trials within 15 years [17]. In 2014, Switzerland expanded i-voting to all Swiss abroad but imposed increasingly stringent security standards. Despite operational success, persistent concerns about vulnerabilities led to the halting of broader rollout plans by 2019, particularly following critical flaws discovered in Swiss Post's system [17]. In response, authorities initiated a comprehensive redesign. As of 2023, Switzerland cautiously resumed trials under tightened conditions [18].

4.3.1 Data Privacy Techniques

Federal regulations mandate that "no one should know how a voter voted" [19]. Accordingly, all ballots are end-to-end encrypted, and cryptographic protocols decouple voter identity from the ballot. Systems employ techniques such as mixnets and distributed decryption across multiple independent authorities [19].

A notable innovation is the use of return codes: voters receive a paper code sheet via postal mail. After voting online, a system-generated return code allows voters to verify, in real time, that their encrypted vote matches their intended selection, without revealing the choice to others [19]. These verification codes safeguard against malware on voting devices and are now a compulsory feature under federal regulations.

4.3.2 Verification and Vote Integrity

Swiss i-voting emphasizes end-to-end verifiability: both voters and auditors must be able to independently verify the election outcome. Individual verifiability allows each voter to confirm their ballot was cast as intended using return codes [19]. Swiss Post's system, sVote, enforces this through unique printed choice codes.

At the same time, universal verifiability ensures that all votes are recorded and tallied correctly. Cryptographic proofs, including

zero-knowledge proofs generated during Mixnet shuffling and decryption, are publicly released, allowing external audits [18]. As of 2022, only fully verifiable systems meeting both individual and universal verifiability criteria are authorized for use [18].

4.3.3 Transparency and Open Source Practices

Geneva's CHVote project was eventually open-sourced [16], while Swiss Post shifted to a "systematic transparency strategy" post-2019, releasing core cryptographic protocols and verification tools as open source [18].

Moreover, public bug bounty programs and penetration tests, such as the 2019 intrusion test, have been institutionalized to detect vulnerabilities [20, 21]. Technical documentation and system updates are also made public to promote accountability and scrutiny. Federal regulations now mandate open-source practices and independent academic reviews before new trials [18].

4.3.4 Vulnerabilities and Privacy Concerns

Despite precautions, Swiss i-voting trials revealed serious vulnerabilities. In 2019, researchers uncovered a critical flaw in Swiss Post's system, allowing undetectable vote manipulation via an error in the zero-knowledge proof [20, 21]. Consequently, the Swiss Post's system was withdrawn from elections, and broader i-voting expansion was halted [17].

The Geneva CHVote system also suffered from critical flaws, with research identifying nine potential attack vectors [19]. These findings underscored the inherent difficulty of achieving perfect security in online voting systems. Although no actual breaches occurred, the theoretical risks demonstrated the necessity of Switzerland's cautious trial-based approach.

Broader concerns, such as client-side malware, insider threats, and mass surveillance potential, remain salient. While Swiss systems mitigate these risks through encryption, return codes, and distributed trust, critics argue that vulnerabilities in voters' devices remain a persistent challenge.

4.3.5 Public Perception and Trust

Public opinion on i-voting in Switzerland is divided. Expatriate communities and advocacy groups for people with disabilities support i-voting for its convenience and accessibility [17]. However, security incidents have fueled public skepticism. Initiatives advocating for a moratorium or permanent ban on e-voting have emerged, citing the inherent insecurity of online voting [17].

Surveys suggest that while 65-70% of citizens are open to i-voting under robust safeguards, a vocal minority remains opposed. Transparency initiatives, including public audits and educational outreach, aim to rebuild trust. Yet, widespread acceptance depends on maintaining a flawless security track record and ongoing public engagement.

4.4 Estonian I-Voting System

Following its re-establishment as an independent state in 1991 and the potential of digital infrastructure for governance, the Estonian government launched a series of e-governance initiatives under the broader concept of "e-Estonia." By the late 1990s, services provided by government offices were starting to be digitized on the e-Estonia platform, such as declaring taxes [22] .

In 2001, the Estonian Parliament amended its electoral laws to permit electronic voting, laying the legal foundation for internet voting. Estonia with a population of approximately 1.3 million became the first nation to implement legally binding nationwide Internet voting starting with 2005's local elections.

4.4.1 Voting Procedure

Estonia's internet voting system is built upon the country's national digital identity infrastructure. Each citizen is issued an ID card containing two encrypted digital certificates: one for authentication and another for digital signatures.

Voting is conducted through a secure application downloadable from the official election website, Valimised.ee. During the designated pre-voting period, which begins on Monday and concludes on Saturday evening of the voting week, eligible voters authenticate themselves using their ID cards or Mobile-ID credential [23].

Voters are permitted to cast multiple votes during the pre-voting period, with only the final submission being considered valid; previous digital votes are automatically annulled. Additionally, voters retain the option to vote in person using a paper ballot on election day on Sunday, which will nullify any prior electronic vote.

To ensure individual verifiability, voters may utilize the EH Kontrollrakendus verification application developed by Cybernetica AS and available through the App Store and Google Play Store [24]. Once the vote is cast, a unique QR code is generated by the voting system. Using their identification credentials and the QR code, voters can confirm that their vote was successfully received and correctly attributed.

4.4.2 Vote Processing

Once the voting period concludes, electronic votes undergo a two-phase processing procedure. In the initial phase, duplicate i-votes and those associated with voters who also cast paper ballots are identified and excluded. For the remaining valid i-votes, digital signatures are detached to ensure voter anonymity. The encrypted votes are then subjected to a mixing process, during which the order of votes is randomized. This step is accompanied by a cryptographic mixing proof to certify that no votes were altered, added, or removed [25].

In the second phase, the encrypted votes are decrypted using a private key, which is distributed among members of the National Electoral Committee. All segments of the key must be combined to enable decryption. Subsequently, votes are tallied and matched to candidates. The system generates a tallying proof to validate the accuracy of the results and to support post-election audits [25].

The processed results are compared with those from election day for verification purposes. Both electronic and paper ballots are retained for one month to accommodate potential legal challenges. Following the resolution of any disputes and the formal declaration of the election results, all votes are securely destroyed to uphold voter anonymity [25].

4.4.3 Data Privacy Techniques

The Estonian i-voting protocol employs several cryptographic techniques, including public-private key encryption, a double envelope model, and verifiable mixing and tallying processes. The system relies on the ElGamal cryptosystem, a non-deterministic and homomorphic encryption method, to generate secure key pairs for each vote.

After a voter selects a candidate, their vote is encrypted and encapsulated within a digital ballot creating the inner envelope. This is then signed with the voter's digital signature to form the outer envelope. The use of separate envelopes facilitates both voter authentication and ballot anonymity.

Cryptographic proofs are automatically generated during the vote mixing and tallying stages using software such as Verificatum, which is designed for secure election counting [26]. The mixing proof ensures the integrity of the randomized vote order, while the tallying proof confirms the accuracy of the final count.

4.4.4 Anonymity and Individual Verifiability

To maintain unlinkability between voters and their selections, Estonia employs a combination of the double envelope method and the vote mixing process. Individual verifiability is enabled through the use of a QR code and the EH Kontrollrakendus application, allowing voters to confirm that their vote was registered correctly and associated with the intended candidate [23].

4.4.5. Vulnerabilities and Privacy Concerns

When internet voting was first established in 2005 for the municipality elections, Arnold Rüütel, the President of Estonia at the time, petitioned against internet voting on the grounds of internet voting disrupting the principle of uniformity. He claimed that the possibility to change the given internet vote for an unlimited number of times creates a disadvantage for voters casting their ballot in other voting channels. The Supreme Court of Estonia has dismissed the petition [27].

The elections are closely inspected by cybersecurity researchers as Springall et. al. (2014) criticised the lack of transparency on vote processing, insecure voting software downloads and vulnerabilities in published source code [28].

4.4.6 Voter Participation and Public Trust

In the 2005 local elections, internet voting constituted only 1.9% of the total votes cast. By the 2023 parliamentary elections, this figure had risen to over 51%, marking the first instance in which a majority of votes were submitted online . Estonia remains the only nation to have implemented nationwide internet voting on a consistent basis, maintaining both legal recognition and public trust for over a decade.

The Estonian elections have been closely inspected by OSCE, Organization for Security and Cooperation in Europe and their reports suggest that the current voting system is aligned with international standards [29].

5 Criteria

In this section, we outline the criteria selected for our framework and their rationale. Our framework evaluates i-voting systems based on voter participation, computational cost, anonymity, availability, resilience and transparency. Each criterion is detailed in the following subsections.

5.1.1 Voter Participation

Voter turnout has declined in recent years, encouraging many countries to seek improvements. Internet voting represents one potential solution by enhancing accessibility. Research presents mixed findings regarding the relationship between i-voting and participation rates. Some suggest that the availability of i-voting systems increases voter turnout, whereas others imply that there is no causal relationship between i-voting systems and voter turnout [30].

This criterion is significant for our framework because the connection between i-voting and voter participation is more nuanced than initially apparent. Participation rates depend not only on voting methods but also on public trust in the i-voting system and the prevailing political climate [30]. While political circumstances cannot be directly compared, examining turnout across different countries provides valuable insights into their respective internet voting systems.

5.1.2 Computational Cost

Traditional polling station voting costs include stationary materials, hardware systems, and personnel requirements. Internet voting systems, however, necessitate additional consideration of computational expenses [31]. The algorithms employed and their

implementation affect time efficiency and, consequently, the system's computational cost.

This criterion is essential for a data privacy framework as computationally intensive systems may prove impractical in real-world applications. Therefore, finding an appropriate balance between data privacy and cost efficiency is crucial.

5.1.3 Anonymity

Elections require all voters to be eligible participants. Traditional voting systems verify eligibility through administrative staff, while remote internet voting systems employ varied verification methods. Switzerland uses physical identification cards, whereas Estonia employs digital IDs [32].

Beyond eligibility, votes must be verified without compromising voter identity. Norway addresses this by sending verification codes via message [6], Switzerland posts verification codes that must match ballots [33], and Estonia permits multiple votes where each submission invalidates the previous one, and the last vote is counted as the valid one. Each system employs distinct methods to maintain voter privacy while preserving electoral integrity. Consequently, anonymity represents a vital criterion for any privacy framework.

5.1.4 Availability and Resilience

Our next criterion concerns availability and resilience—the system's ability to function properly despite potential attacks on the server. Many countries utilize distributed servers to divide responsibilities, implementing separation of duty for voting servers. To further enhance resilience, they employ multiple control functions, such as parallel tallying processes [34].

A voting system's resilience is fundamental, as it must operate effectively even when components are compromised. Therefore, availability and resilience are essential elements of our privacy framework for evaluating i-voting systems.

5.1.5 Transparency

Our final criterion addresses the transparency of Internet voting systems. A system's transparency directly influences public trust and consequently affects voter participation. Some nations discontinued i-voting initiatives due to low public confidence. To address this concern, countries like Switzerland and Estonia have released older system versions as open source. Furthermore, most i-voting systems incorporate vote verifiability, enabling voters to confirm their votes were correctly recorded. This verification capability enhances process transparency by providing voters with direct confirmation mechanisms. We consider transparency an essential element for any privacy-preserving internet voting system.

5.2 Criteria Pointing System

Criteria	Voter Participation	Computational Cost	Anonymity	Availability and Resilience	Transparency
Range	0-10	0-10	0-10	0-10	0-10
Weight	20%	15%	30%	15%	20%

Table 1: *Range and weight of each criterion*

5.2.1 Weights

- **Anonymity (30%)**

Protecting voter privacy is the core objective of any i-voting system. A breach in anonymity not only undermines individual secrecy but can also cascade into broader trust and legal failures. Hence, it carries the highest weight.

- **Voter Participation (20%)**

One of the main motivations for Internet voting is to increase turnout. We assign substantial emphasis to this criterion because a technically secure system still might have limitations if the usage remains negligible.

- **Transparency (20%)**

Open processes and auditability directly feed public confidence. Transparency enables third-party review, bug bounties, and legal accountability, all of which reinforce both security and participation.

- **Computational Cost (15%)**

While security and privacy often demand expensive cryptography, excessive computational burden can render a system economically unviable for large-scale elections. Thus, cost is important but secondary.

- **Availability & Resilience (15%)**

A system must remain alive and correct under real-world conditions (e.g., DoS attacks and server failures). We weigh this on par with cost, as both operational continuity and budget constraints are practical considerations.

5.2.2 Scoring Ranges

Every criterion is normalized to 0–10 to allow direct comparison and weighted aggregation.

- **Voter Participation**

Scored by multiplying the percentage of total votes cast online by 10 (e.g., Estonia's ~50 % ⇒ 5.0).

- **Computational Cost**

Cost per voter mapped to the 0–10 scale (lower USD/voter ⇒ higher score). For instance, a $1-2/vote cost earned France a 9, while Estonia's $4/vote scored 8.

- **Anonymity**

Evaluated qualitatively based on protocol design (e.g., mix-nets, double-envelopes) and practical vulnerabilities (e.g., client-side malware, potential collusion). Switzerland's robust proofs scored 9, France's flawed linkage scored 2.

- **Availability and Resilience**

Assessed via system architecture (distributed servers, failover) and real-world testing (e.g., Estonia's post-2007 reforms vs. Norway's limited pilots). Scores ranged from 3 (France) to 9 (Switzerland).

- **Transparency**

Based on open-source practices, public audits, and legal frameworks. Switzerland's full openness scored 10; France's closed, obfuscated code scored 1.

6 Evaluations & Results

Our comparison of online voting systems in Estonia, Norway, France, and Switzerland revealed important distinctions as well as noteworthy information on their practical difficulties, privacy protections, security flaws, and operational efficacy.

Estonia's system, active since 2005, uses digital ID cards and a revoting mechanism to mitigate coercion risks, though client-side malware remains a persistent vulnerability. Norway's system applied strong cryptographic protections, including ElGamal encryption and threshold cryptography, but was discontinued in 2014 due to political concerns and privacy risks arising from potential collusion between critical system components and insecure verification channels. France's Neovote platform, introduced during the COVID-19 pandemic, suffered from significant privacy weaknesses, including closed-source development, outdated cryptographic practices, and susceptibility to MITM attacks, despite its formal compliance with national cybersecurity standards. Switzerland adopted a decentralized, transparency-focused model using end-to-end encryption, mixnets, and return-code verification, but critical cryptographic vulnerabilities discovered in 2019 led to a temporary suspension and stricter regulatory reforms emphasizing open-source development and public auditing.

Criterion	Estonia	Norway	France	Switzerland
System Status	Active	Stopped (2014)	Active (limited confidence)	Restarted (limited scope)
Authentication	Digital ID	SMS/Postal Verification	Username/Password	Postal Return Codes
Main Privacy Strength	Revoting mechanism	Threshold cryptography	CNIL and ANSSI cybersecurity standarts	End-to-end encryption
Major Privacy Weakness	Client-side risks	BB & RG collusion	Weak cryptography, MITM risks	Client-side malware risks
Transparency Level	Medium	Medium	Very Low	High

Table 2: *Overall view of i-voting systems in Estonia, Switzerland, France, and Norway*

6.1 Evaluation

Criteria \ Country	Voter Participation	Computational Cost	Anonymity	Availability and Resilience	Transparency
Estonia	5	8	8	8	6
Norway	3.5	6	7	5	5
France	0.14	9	2	3	1
Switzerland	2.5	5	9	9	10

Table 3: *Evaluation of Estonia, Switzerland, France, and Norway regarding our criteria*

6.1.1 Voter Participation Evaluation

In our voter participation evaluation, we directly scaled the participation rates of each country to a 0-10 scale, where a 100% participation rate corresponds to the maximum score of 10. This means that the actual percentage of the population using internet voting was multiplied by 10 to determine the final score. Estonia, with approximately 50% participation, scored 5.0; Norway, with 35% participation, scored 3.5; Switzerland, with 25% participation, scored 2.5; and France, with 1.4% participation, scored 0.14. This approach focuses purely on the relative adoption of internet voting within each country, allowing for a clear and proportional comparison across systems regardless of absolute population size.

6.1.2 Computational Cost Evaluation

An important consideration when assessing the economic feasibility and scalability of online voting systems is computational cost. Systems that place a high priority on data privacy, transparency, and verifiability are, by nature, more computationally demanding, which frequently results in greater costs. However, if these expenses are necessary to protect voter privacy and election integrity, they may be justified for national elections.

Estonia has achieved an optimal balance between cost-efficiency and privacy, with an estimated cost of about 4 USD per voter [35], supporting a sustainable nationwide system and earning it a score of 8. Norway, while securing strong cryptographic protections using homomorphic encryption and zero-knowledge proofs, incurred an estimated 20 USD per voter [36], resulting in a lower practicality score of 5 despite excellent privacy guarantees. Switzerland's decentralized system focusing on full end-to-end verifiability imposes high computational demands, estimated at around 10–15 USD per voter [37], justifying a moderate score of 6. France's Neovote platform, employing outdated and less secure cryptographic methods, achieved the lowest costs at around 1–2 USD per voter [38], but sacrificed essential security principles, resulting in a score of 9.

6.1.3. Anonymity Evaluation

Anonymity ensures that votes cannot be traced back to individual voters. In evaluating anonymity, we considered both the protocol design and the practical risks introduced by client devices or potential insider threats, as well as historical attack incidents and public vulnerabilities.

Estonia's system exhibits strong anonymity because of its verifiable mixing mechanism and double-envelope concept. Votes are cryptographically separated from voter identities following authentication, offering a high degree of unlinkability. However, its score is lowered to 8 due to residual hazards associated with client-side malware. Notably, a 2014 independent security analysis revealed vulnerabilities that could potentially allow compromised voter devices to alter votes before encryption without voter awareness, thereby indirectly impacting anonymity through device-level attacks.

Norway's method provides high theoretical anonymity by using threshold cryptography, return codes, and homomorphic encryption. However, a score of 7 reflects the non-negligible danger of cooperation between internal system components (the Ballot Box and Receipt Generator). Formal analyses acknowledged that collusion could, under specific conditions, reconstruct decrypted votes. Although no actual breaches were reported during Norway's pilot elections, this structural weakness remains a theoretical but critical anonymity concern.

Switzerland's internet voting design provides the strongest anonymity protections among the evaluated systems, leveraging public cryptographic verifiability, distributed trust models, and end-to-end return code verification. In 2019, however, researchers discovered critical flaws in Swiss Post's zero-knowledge proofs, which could have enabled undetectable manipulation of votes without breaching anonymity directly. Despite the severity of this flaw, there was no public indication of actual deanonymization. Therefore, Switzerland maintains a high anonymity score of 9, with minor risks primarily associated with client device malware.

In contrast, France's Neovote system suffers from significant anonymity weaknesses. Votes and receipts are not securely linked, the system is closed-source, and independent verifiability is absent, leading to a very low score of 2. Furthermore, reverse engineering efforts revealed the use of outdated cryptographic libraries (asmcrypto.js) and poor randomness sources in mobile clients. These weaknesses could theoretically expose vote content or allow attackers to manipulate votes, undermining both anonymity and system integrity. No large-scale breaches have been officially confirmed, but the technical flaws indicate systemic vulnerabilities that could easily lead to deanonymization in real-world deployments.

6.1.4. Availability and Resilience Evaluation

Both the election's dependability and voter confidence are seriously damaged if an electronic voting system malfunctions, stops working, or is not resilient enough to resist cyberattacks such as denial-of-service (DoS) attacks. Voter participation rates are, therefore, almost as crucial as the system's resilience to attacks and ability to bounce back from setbacks.

Estonia's system demonstrates strong availability through its distributed server architecture, redundancy strategies, and well-planned failover mechanisms. Despite the little risk associated with relying on voting equipment, Estonia's infrastructure is very robust overall. The nation's internet services were severely disrupted by the 2007 cyberattacks, which prompted significant reforms and investments in distributed, fault-tolerant architectures that are still advantageous for i-voting systems today. Estonia thus has an excellent availability and resilience score of 8.

Norway's i-voting system was theoretically designed to be resistant to collusion, using threshold cryptography and distributed key management. But it did so only in a few small pilot tests, without the pressure of real-world, large-scale attacks. Internally, it was believed that such a facility might have been susceptible to a severe denial-of-service attack because of a

relatively centralized architecture. As a result, Norway is moderately scored, receiving a 5, in that it is untested in response to real-world attacks.

Switzerland's decentralized canton-based deployment model offers the highest resilience among the countries evaluated. Because each canton functions independently, localized failures can be isolated without affecting the outcome of the national election. Authorities proactively suspended online voting trials in 2019 after vulnerabilities in Swiss Post's e-voting system were discovered during public penetration testing. Switzerland's prompt and open response to vulnerabilities shows excellent resilience management, even though no real attacks interfered with the voting process. This explains why the resilience score of nine is so high.

On the other hand, the Neovote platform from France exhibits notable shortcomings in terms of availability and resilience. Without enough public transparency, the system is dependent on a centralized, opaque infrastructure. The vote verification system is extremely susceptible to denial-of-service attacks, according to security audits conducted in 2022 and 2023. The system's vulnerability was exposed when verification tools crashed under extreme load. System availability is severely harmed by this verified vulnerability to DoS attacks, earning it a low score of 3.

6.1.5 Transparency Evaluation

Estonia achieves moderate transparency by publicly disclosing protocol specifications and cryptographic models. However, the core server-side code remains closed-source, limiting full external verification. Consequently, Estonia receives a transparency score of 6.

Norway also demonstrates a medium level of transparency. Detailed protocol descriptions and formal security analyses were made publicly available during the i-voting trials. However, the source code of core components and operational procedures were not fully open, leading to a similar score of 5.

Switzerland's approach sets the benchmark for transparency. Following the discovery of vulnerabilities in 2019, Swiss authorities mandated that e-voting systems must be fully open-source, subjected to independent academic reviews, and tested through public bug bounty programs [39]. This comprehensive transparency framework justifies Switzerland's high score of 10.

In stark contrast, France's Neovote system exhibits severe transparency deficiencies. The platform remains closed-source with obfuscated client-side code, blocking meaningful third-party analysis. Security audits revealed significant barriers to independent verification, resulting in a low transparency score of 1.

6.2 Results

After calculating the overall score of each country with this formula Total Score: (VP×0.20)+(CC×0.15)+(A×0.30)+(AR×0.15)+(T×0.20). We obtain the following table:

Criteria \ Country		Total Score out of 10
Estonia	(5×0.20)+(8×0.15)+(8×0.30)+(8×0.15)+(6×0.20)	7.0
Norway	(3.5×0.20)+(6×0.15)+(7×0.30)+(5×0.15)+(5×0.20)	5.45
France	(0.14×0.20)+(9×0.15)+(2×0.30)+(3×0.15)+(1×0.20)	2.63
Switzerland	(2.5×0.20)+(5×0.15)+(9×0.30)+(9×0.15)+(10×0.20)	7.3

Table 4: *Total scores of each country regarding our weighted criteria*

After evaluating four countries based on five main criteria: voter turnout, processing costs, anonymity, usability and durability, and transparency. Switzerland came out on top with an overall score of 7.3 out of 10. Their strong focus on auditability, clear transparency practices, and system resilience makes this implementation more preferable. Estonia earns a score of 7.0 due to their well-balanced design that combines efficiency, scalability, and privacy protection, but there are still some minor security risks to voters' personal devices. Norway follows with 5.45 points; while its cryptographic foundation is solid, limited real-world implementation and moderate durability issues have held it back. Lastly, France scored the lowest at 1.73, largely due to a lack of transparency, outdated cryptographic practices, and security vulnerabilities that threaten both privacy and system stability. Overall, while no system is perfect, this comparison demonstrates how important transparency, public verifiability, and resilience to real-world threats are in building trustworthy online voting systems.

7 Proposed Privacy Framework

Based on the comparative analysis of Estonia, Switzerland, Norway, and France, we propose a privacy-focused evaluation framework that defines minimum acceptable scores (0–10 scale) for each key criterion, along with ideal targets. This framework ensures that an i-voting system meeting these benchmarks can be deemed sufficiently privacy-preserving. We also establish an overall minimum weighted score (using the existing weightings in Table 1) required for a system to be considered acceptable.

7.1 Voter Participation

Minimum Acceptable Score: 5/10. We require at least a 5 on the 0–10 scale (approximately 50% of votes cast online) to ensure the system achieves significant user adoption because even technically robust implementations become irrelevant without substantial voter engagement. Empirical evidence from case studies supports this threshold: Estonia's sustained adoption rate of approximately 50% (score ~5.0) illustrates successful public acceptance, whereas Norway's discontinued trials, with 35% participation (score 3.5), reveal the consequences of moderate but insufficient engagement. Conversely, France's 2020s implementation achieved merely 1.4% online turnout (score 0.14), underscoring the risks of deploying systems that fail to gain traction. The 5/10 minimum thus functions as a safeguard, ensuring that i-voting systems are not only operationally sound but also democratically consequential by requiring demonstrable voter confidence and utilization. This criterion aligns with broader democratic principles, as participation levels directly reflect public trust and the perceived legitimacy of digital voting infrastructure.

7.2 Computational Cost

Minimum Acceptable Score: 6/10. We recommend at least a 6 on cost-efficiency, indicating the system's privacy protections do not impose impractical overhead. Internet voting inherently adds cryptographic and infrastructure costs beyond traditional voting [1]. If the cost is too high (low score), nationwide deployment may be unsustainable; if cost is extremely low (high score) due to cutting corners, critical privacy features might be absent. Our case studies show the need for balance. Estonia achieved a score of 8 with an estimated cost of $4 per voter, reflecting a sustainable design that still prioritizes privacy. Switzerland's fully verifiable, privacy-rich system is more expensive ($10–15 per voter) and earned a moderate score ~6. Norway's pilot incurred about ~$20 per voter due to heavy cryptography, yielding a low practicality score (5) despite strong privacy. By contrast, France's system had the cheapest implementation ($1–2 per voter) but "sacrificed essential security principles", earning a cost score of 7 while suffering serious privacy flaws. These examples underscore that neither extreme is ideal: a minimum score of 6 ensures the system is efficient enough for real-world use but not at the expense of privacy. At this threshold, the architecture employs necessary cryptographic protections without becoming prohibitively costly.

7.3 Anonymity

Minimum Acceptable Score: 8/10. This benchmark signifies that only systems employing robust, cryptographically proven safeguards—with strictly limited theoretical vulnerabilities—can be considered viable. Our case studies demonstrate that failure to meet this standard introduces unacceptable privacy risks. Estonia's system, which utilizes double-envelope encryption and mixing mechanisms, achieved a score of 8, reflecting strong anonymity protection despite minor residual risks from potential voter device malware. Norway's implementation, while theoretically sound through return codes and threshold encryption, received a 7 due to a non-negligible insider collusion vulnerability; analyses revealed that coordinated malfeasance between the ballot box and receipt generator could compromise vote secrecy [7]. This flaw, though never exploited, critically undermined confidence in the system. At the opposite extreme, France's closed-source Neovote platform, which relied on obsolete cryptography and lacked independent verifiability, scored only 2—a catastrophic failure that rendered its anonymity protections practically nonexistent [5].

To satisfy the 8/10 threshold, an i-voting system must integrate end-to-end encryption, mixing or homomorphic tallying, distributed trust architectures, and comprehensive auditing to eliminate known deanonymization vectors. Switzerland's redesigned system exemplifies this standard, approaching near-perfect anonymity (9/10) through publicly verifiable cryptography, distributed trust models, and end-to-end return code verification [18, 19]. These implementations underscore that voter anonymity cannot be treated as a secondary consideration; it demands the highest technical and procedural rigor to ensure democratic legitimacy.

7.4 Availability and Resilience

Minimum Acceptable Score: 7/10. This benchmark reflects the necessity for fault-tolerant architectures that maintain service continuity during cyber incidents or technical failures. Estonia's i-voting system exemplifies this standard, having achieved a score of 8 through its distributed server architecture with redundancy mechanisms, which successfully withstood the 2007 nationwide cyberattacks. Subsequent infrastructure investments further enhanced its robustness, establishing a model of adaptive resilience [1]. Switzerland's system demonstrates even greater resilience (score 9), employing a decentralized cantonal structure that isolates potential failures while maintaining system-wide integrity. The Swiss approach to vulnerability management—including the proactive suspension of trials in 2019 to address security flaws—exemplifies best practices in resilience governance [37].

Conversely, France's centralized and non-transparent architecture proved critically deficient, scoring only 3/10 after its verification service collapsed under simulated denial-of-service attacks. Similarly, Norway's pilot system (score 5) incorporated some distributed elements but remained operationally untested against large-scale attacks, raising concerns about its capacity to handle real-world threats [12, 13]. These comparative cases underscore that resilience cannot be an afterthought; systems scoring below 7/10 risk catastrophic failure during electoral operations.

The 7/10 minimum threshold thus ensures that i-voting systems incorporate redundant infrastructure, stress-tested defenses, and contingency protocols sufficient to guarantee continuous availability. This requirement distinguishes sustainable implementations from those vulnerable to disruption, reinforcing the principle that resilience is inseparable from electoral integrity.

7.5 Transparency

Minimum Acceptable Score: 6/10. This benchmark requires that fundamental aspects of the system - including core cryptographic processes and verification mechanisms - be open to examination, either through source code disclosure, third-party audits, or comprehensive procedural oversight. The case studies demonstrate a clear correlation between transparency levels and system viability: France's completely opaque, closed-source implementation (score 1) [5] resulted in such profound distrust that the system became politically untenable, while Norway's partial transparency (score 5), characterized by limited disclosures and vendor dependence, ultimately contributed to the project's cancellation despite its technical sophistication. Estonia's evolutionary approach illustrates how incremental transparency improvements can build legitimacy. After initial criticisms, the system achieved a score of 6 through selective code releases and regular independent audits [25], demonstrating that even moderated transparency - when combined with other safeguards - can sustain public confidence. Switzerland's model (score 10) represents the gold standard, with complete open-source disclosure and public penetration testing establishing unparalleled verifiability [16].

The 6/10 minimum threshold thus balances practical implementation constraints with democratic accountability requirements. It ensures that while not every component need be publicly accessible, sufficient mechanisms exist for: independent verification of critical security claims, detection of potential malfeasance and voter-accessible confirmation of proper ballot handling. This standard acknowledges that in electoral systems, transparency serves not merely as an ideal but as a necessary precondition for maintaining public trust in the democratic process. Systems falling below this threshold risk losing legitimacy regardless of their technical merits, as evidenced by the comparative failures of more opaque implementations.

7.6 Overall Minimum Score

Minimum Acceptable Total: 6.0/10 (weighted). In addition to per-criterion requirements, we propose that an internet voting system must achieve an overall weighted score of at least 6.0 out of 10 under our criteria weighting scheme. Requiring a composite score ≥6.0 ensures balanced performance – the system cannot fall too far behind in any one area without jeopardizing the overall evaluation. Notably, Norway's system scored 5.45/10 overall as seen in Table 4, which falls below our proposed minimum, and ultimately Norway did not continue its i-voting program. France's system, with an overall around 2 out of 10, was clearly unacceptable – its severe transparency and anonymity failures dragged its total score down, exemplifying why a strong aggregate score is needed. In contrast, Estonia and Switzerland both exceeded this threshold with overall scores of 7.0 and 7.3, respectively. These higher scores align with real-world success: Estonia's and Switzerland's systems have been deployed over multiple election cycles, suffering only manageable issues.

By setting 6.0 as the required floor, we ensure that a system must perform decently across all dimensions of privacy and trust. As a point of reference, a truly robust i-voting system in the future might score 8+ out of 10 overall, reflecting excellence in most criteria. Our minimum of 6.0 simply marks the lowest acceptable composite score for real-world deployment; any lower, and the system's privacy posture is too weak to inspire sufficient trust.

Criterion	**Weight**	**Minimum Acceptable Score (0–10)**
Voter Participation	20%	5/10 (~50% online voting)
Computational Cost	15%	6/10
Anonymity	30%	8/10
Availability & Resilience	15%	7/10
Transparency	20%	6/10
Overall Weighted Total	—	**≥ 6.0 / 10**

Table 5: *Minimum acceptable score for each criterion according to the proposed privacy framework*

8 Conclusion and Future Work

This study presents a comparative evaluation of i-voting systems in Estonia, Switzerland, Norway, and France, with a focus on data privacy techniques. We assess each system across: voter participation, computational cost, anonymity, availability, resilience, and transparency. By analyzing documented vulnerabilities, privacy safeguards, operational histories, and real-world outcomes, we propose a privacy framework that sets minimum acceptable scores for each criterion, requiring an overall weighted score of at least 6.0 out of 10 for a system to be deemed sufficiently privacy-preserving.

Our findings reveal that robust data privacy in i-voting extends beyond cryptographic security. Real-world resilience, transparent verifiability, sustainable operational costs, and public trust are equally critical. Estonia and Switzerland demonstrate how a cautious, open, and verifiable approach fosters trust and system robustness. Conversely, France's experience highlights the dangers of compromising transparency and cryptographic rigor, while Norway's trials show that even technically sound systems can falter without real-world resilience and broad adoption.

The proposed framework ensures no single privacy or trust dimension is overlooked. Systems must meet baseline scores in all five criteria while maintaining an acceptable overall performance—only then can they be considered viable for democratic use.

While this study establishes a structured assessment model, future research should refine and expand it. Potential directions include:

- Dynamic, context-sensitive scoring models that adjust thresholds based on election types (e.g., national vs. local) or threat landscapes.
- Integration of adversarial testing results, such as stress tests or formal security audits, as additional evaluation criteria.

In conclusion, this framework provides a systematic, balanced approach to developing and evaluating privacy-preserving i-voting systems, ensuring they meet the stringent demands of democratic integrity.

REFERENCES

[1] J. Udris and I. Groza, Feasibility Study on Internet Voting for the Central Electoral Commission of the Republic of Moldova: Report and Preliminary Roadmap, United Nations Development Programme in Moldova, Chisinau, Moldova, Version of 28/06/2016.

[2] "Electronic Voting in the United States and Estonia," Legislative Council of the Hong Kong Special Administrative Region – Research Publication Database, https://app7.legco.gov.hk/rpdb/en/uploads/2023/IN/IN14_2023_20230703_en.pdf (accessed Apr. 7, 2025).

[3] S. Heiberg, P. Laud, and J. Willemson, "The application of I-voting for Estonian parliamentary elections of 2011," in E-Voting and Identity (Vote-ID 2011), A. Kiayias and H. Lipmaa, Eds., Lecture Notes in Computer Science, vol. 7187, Berlin, Heidelberg: Springer, 2012, pp. 208–223. [Online]. Available: https://doi.org/10.1007/978-3-642-32747-6_13

[4] A. Rodríguez-Pérez and J. Puiggalí, Defining a national framework for online voting and meeting its requirements: The Swiss experience, Oct. 2, 2018.

[5] E. Blanchard, A. Gallais, E. Leblond, D. Sidhoum-Rahal, and J. Walter, "An analysis of the security and privacy issues of the Neovote online voting system," in Electronic Voting. E-Vote-ID 2022, R. Krimmer, M. Volkamer, D. Duenas-Cid, P. Rønne, and M. Germann, Eds., Lecture Notes in Computer Science, vol. 13553, Cham, Switzerland: Springer, 2022, pp. 3–21. doi: 10.1007/978-3-031-15911-4_1.

[6] I. S. G. Stenerud and C. Bull, "When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting," Norwegian Ministry of Local Government and Regional Development, Oslo, Norway, 2011.

[7] Ministry of Local Government and Modernisation, "Internet voting trials," Government.no, https://www.regjeringen.no/en/topics/elections-and-democracy/internet-voting-trials/id2666749/ (accessed Apr. 7, 2025).

[8] N. Kaaniche, M. Laurent, and S. Belguith, "Privacy enhancing technologies for solving the privacy–personalization paradox: Taxonomy and survey," J. Netw. Comput. Appl., vol. 171, p. 102807, Aug. 2020, doi: 10.1016/j.jnca.2020.102807.

[9] A. Debant and L. Hirschi, "Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol," in *Proc. 32nd USENIX Security Symposium (USENIX Security 23)*, Anaheim, CA, USA, Aug. 2023, pp. 6737–6752. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/debant

[10] K. Gjøsteen, "The Norwegian Internet Voting Protocol," Lecture Notes in Computer Science, vol. 7187, pp. 1–18, 2012.

[11] V. Cortier and C. Wiedling, "A Formal Analysis of the Norwegian E-voting Protocol," Lecture Notes in Computer Science, vol. 7215, pp. 109–128, 2012.

[12] V. Cortier and C. Wiedling, "A formal analysis of the Norwegian E-voting protocol," Journal of Computer Security, vol. 25, no. 1, pp. 21–57, 2017.

[13] S. Kardaş, M. S. Kiraz, M. A. Bingöl, and F. Birinci, "Norwegian internet voting protocol revisited: Ballot box and receipt generator are allowed to collude," Security and Communication Networks, vol. 9, pp. 5051–5063, 2016.

[14] Serdult, Uwe (2015). "Fifteen years of internet voting in Switzerland [History, Governance and Use]". 2015 Second International Conference on e Democracy & e Government (ICEDEG). IEEE. pp. 126–132. doi:10.1109/ICEDEG.2015.7114482. ISBN 978-3-9075-8910-6. S2CID 7735114.

[15] "Wahlbeteiligung," Statistik Schweiz - Wahlbeteiligung, https://web.archive.org/web/20121116080733/http://www.bfs.admin.ch/bfs/portal/de/index/themen/17/02/blank/key/national_rat/wahlbeteiligung.html (accessed Apr. 25, 2025).

[16] Republique-Et-Canton-De-Geneve, "Republique-et-Canton-de-Geneve/chvote-1-0: The Geneva Electronic Vote system, version 1.," GitHub, https://github.com/republique-et-canton-de-geneve/chvote-1-0 (accessed Apr. 25, 2025).

[17] U. Geiser, "E-voting suffers another setback amid expat Swiss concerns," SWI swissinfo.ch, https://www.swissinfo.ch/eng/politics/digital-democracy_e-voting-suffers-another-setback-amid-expat-swiss-concerns/45059918 (accessed Apr. 25, 2025).

[18] D. S. Post, "E-voting – electronic vote casting for Switzerland," Swiss Post, https://www.post.ch/en/about-us/profile/swiss-post-and-politics/swiss-post-in-the-digital-world/e-voting-electronic-vote-casting-for-switzerland (accessed Apr. 25, 2025).

[19] V. Cortier, A. Debant, and P. Gaudry, IACR, https://eprint.iacr.org/2025/080.pdf (accessed Apr. 25, 2025).

[20] K. Zetter, "Experts find serious problems with Switzerland's online voting system before public penetration test even begins," VICE, https://www.vice.com/en/article/experts-find-serious-problems-with-switzerlands-online-voting-system-before-public-penetration-test-even-begins/ (accessed Apr. 25, 2025).

[21] K. Zetter, "Researchers find critical backdoor in Swiss online voting system," VICE,

https://www.vice.com/en/article/researchers-find-critical-backdoor-in-swiss-online-voting-system/ (accessed Apr. 25, 2025).
[22] e-Estonia, "Story," *e-Estonia*, 2022. [Online]. Available: https://e-estonia.com/story/
[23] "Documents about Internet Voting | Elections in Estonia," Valimised.ee, 2025. https://www.valimised.ee/en/internet-voting/documents-about-internet-voting (accessed Apr. 28, 2025).
[24] Riigikogu Kantselei, "EH kontrollrakendus," Google.com, 2021. https://play.google.com/store/apps/details?id=ee.ivxv.ivotingverification&hl=tr (accessed Apr. 28, 2025).
[25] "Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel Tallinn 2023." Accessed: Apr. 28, 2025. [Online]. Available: https://www.valimised.ee/sites/default/files/2023-02/General%20description%20of%20the%20framework%20of%20the%20i-voting%20system%20%E2%80%9CIVXV%E2%80%9D%20%28in%20Estonian%29.pdf
[26] Verificatum.com, 2025. https://www.verificatum.com/ (accessed Apr. 28, 2025).
[27] "Constitutional judgment 3-4-1-13-05 | The Estonian Supreme Court," Riigikohus.ee, 2025. https://www.riigikohus.ee/en/constitutional-judgment-3-4-1-13-05 (accessed Apr. 28, 2025).
[28] D. Springall et al., "Security Analysis of the Estonian Internet Voting System," Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14, 2014, doi: https://doi.org/10.1145/2660267.2660315.
[29] "Office for Democratic Institutions and Human Rights ESTONIA PARLIAMENTARY ELECTIONS 5 March 2023 ODIHR Election Expert Team Final Report," 2023. Accessed: Apr. 28, 2025. [Online]. Available: https://www.osce.org/files/f/documents/f/f/551179_0.pdf
[30] M. Germann and U. Serdült, "Internet voting and turnout: Evidence from Switzerland," Electoral Studies, vol. 47, pp. 1–12, 2017, doi: 10.1016/j.electstud.2017.03.001.
[31] R. Krimmer, D. Duenas-Cid, and I. Krivonosova, "New methodology for calculating cost-efficiency of different ways of voting: Is internet voting cheaper?" Public Money & Management, vol. 41, no. 1, pp. 17–26, 2021, doi: 10.1080/09540962.2020.1732027.
[32] A. Lust, "I-vote, therefore I am? Internet voting in Switzerland and Estonia," The SAIS Review of International Affairs, vol. 38, no. 1, pp. 65–79, 2018. [Online]. Available: https://www.jstor.org/stable/27001472.
[33] A. Rodríguez-Pérez, J. Cucurull, and J. Puiggalí, "Voter authentication in remote electronic voting governmental experiences: Requirements and practices," in Electronic Participation. ePart 2022, R. Krimmer et al., Eds., Lecture Notes in Computer Science, vol. 13392, Cham, Switzerland: Springer, 2022, pp. 3–15. doi: 10.1007/978-3-031-23213-8_1.
[34] M. Volkamer and R. Grimm, "Determine the resilience of evaluated Internet voting systems," in Proc. 1st Int. Workshop Requirements Engineering for e-Voting Systems (RE-VOTE), Atlanta, GA, USA, 2009, pp. 47–54, doi: 10.1109/RE-VOTE.2009.2.
[35] T. Vassil, "Estonian Internet Voting: Model and Experience," Digital Transformation and Global Society (DTGS), 2016.
[36] Ministry of Local Government and Modernisation, "Norwegian Internet Voting Trials Report," 2014.
[37] Swiss Post, "E-Voting System Transparency Report," 2020
[38] U.S. Election Assistance Commission, "Internet Voting Feasibility Study," 2007.
[39] Swiss Post, "Swiss Post Bug Bounty," *Swiss Post*, [Online]. Available: https://www.post.ch/en/about-us/responsibility/swiss-post-bug-bounty. [Accessed: 28-Apr-2025].