ONLINE VOTING SYSTEM ROADMAP

This procedure assumes the system is **limited** to specific, pre-verified groups (e.g., NRIs, Armed Forces) and is **not** open to the general population, who would still vote in person.

Phase I: Pre-Election (One-Time Registration)

Before an election is even announced, an eligible voter must opt-in to the remote voting system. This cannot be done on polling day.

1. **Eligibility:** The voter must be (a) a registered voter with an **Election Photo ID Card (EPIC)** and (b) belong to a legally defined "remote voter" category (e.g., NRI, active-duty soldier).
2. **Access the Secure ECI Portal:** The voter accesses a dedicated, high-security ECI registration portal.
3. **Initial Authentication:** The voter must prove their identity. This requires:
   - **EPIC Number:** To link to the electoral roll.
   - **Aadhaar Number:** To act as the unique digital identifier.
   - **Proof of Status:** A digital copy of a valid Passport/Visa (for NRIs) or Service ID (for Armed Forces).
4. **Multi-Factor Verification:**
   - An **OTP (One-Time Password)** is sent to the mobile number linked with their Aadhaar.
   - An **OTP** is sent to the mobile number or email linked to their Voter ID record.
5. **Baseline Liveness & Binding:**
   - The voter must perform a **one-time "baseline" liveness check** (e.g., a short video reading a random phrase).
   - This binds their biometrics (face) to their digital profile, which will be used to compare on polling day.
6. **Confirmation & Disqualification:**
   - Once verified, the voter is "locked-in" for remote e-voting.
   - **Crucially, their name is "struck off" the physical electoral roll at their home polling booth.** This makes it *impossible* for them to vote both online and in-person, preventing double voting.

Phase II: Polling Day (The Voting Procedure)

On the designated voting day(s), the voter follows this precise sequence.

Required Items:

- A smartphone or computer with a good internet connection and a working camera/microphone.
- Their pre-registered mobile number (for login OTPs).

- Their Aadhaar-linked mobile number (for Aadhaar OTPs).

Step 1: Login & Authentication

The voter accesses the official ECI Voting App or Web Portal.

1. **Login:** The voter enters their **EPIC Number** (as their username).
2. **First OTP:** An OTP is sent to their **pre-registered mobile number**.
3. **Second OTP:** After entering the first OTP, they must authenticate via Aadhaar. They enter their **Aadhaar number**, and a second, separate OTP is sent to their **Aadhaar-linked mobile**.

This two-OTP process confirms they possess both the number the ECI has on file and the number UIDAI (Aadhaar) has on file.

Step 2: Liveness Verification (The "Digital Booth")

This happens **AFTER** login but **BEFORE** the ballot is shown. This is the most critical step to prevent impersonation.

1. The system activates the device's camera.
2. It issues a **randomized, challenge-response liveness test**. This is not a simple photo.
    - *Example:* "Slowly turn your head to the left," "Read these four numbers (e.g., 8-1-5-2) aloud," or "Blink three times."
3. The system's AI compares the *live video* to the *baseline liveness scan* taken during pre-registration.
4. If it matches, the voter is "cleared" and allowed to proceed. If it fails, they are locked out after 2-3 attempts.

Step 3: Receiving the Anonymous Ballot

1. Once liveness is confirmed, the ECI's "Authorization Server" gives a "green light."
2. A *separate* "Ballot Server" then issues an **anonymous, cryptographically "blinded"** digital ballot to the voter's device.
3. At this exact moment, the system *cryptographically severs* the link between the voter's identity (Voter-XYZ) and the ballot (Ballot-123). The system only knows that Voter-XYZ has been *authorized* to vote, but it cannot see *which* ballot they received.

Step 4: Casting the Vote

1. The voter sees the digital ballot (with party symbols, names).
2. The voter makes their selection.
3. A **Review Screen** appears: "You have selected [Candidate Name / Party Symbol]. Press CONFIRM to cast your vote or BACK to change."
4. **Final Submission:** Upon pressing "CONFIRM," the vote is **homomorphically encrypted on the device itself** *before* being sent over the internet.

Step 5: Confirmation & Verifiable Receipt

1. The encrypted vote is sent to the ECI's "Digital Ballot Box" server.
2. The server receives the encrypted vote and sends back a **confirmation receipt**.
3. This receipt is an **anonymized tracking code** (e.g., a7R-4gT-p9K).

   - **This receipt DOES NOT show the candidate's name.** This is vital to prevent vote-buying and coercion (as the voter cannot *prove* how they voted).

4. The voter can later visit a public "Election Bulletin Board" website, find their tracking code a7R-4gT-p9K on the list, and verify that their encrypted ballot was *included* in the final tally (without revealing *what* was in it).

Phase III: Answering Specific & Judicial Questions

This is how a judge's (or any concerned citizen's) key questions would be answered:

1. Can multiple persons log in from the same device? Yes. The security is tied to the **person**, not the device. A family in the US could use the same laptop. Each voter must log out, and the next voter must start from Step 1, completing their *own* login, their *own* dual-OTP verification, and their *own* individual liveness check.

2. When does liveness detection start? After the initial login (OTP/Aadhaar) but **before** the ballot is issued. This ensures the *authenticated user* is the one *present* for voting. A second, mini-liveness check (e.g., "look at camera") could be added right before final submission.

3. Where is the Election ID Card (EPIC) required? Twice:

1. During the **one-time pre-registration** to link your identity to the electoral roll.
2. As your **primary "username"** when you log in on polling day.

4. How will a Person with a Disability (PwD) vote? This is a profound challenge. The system must be built to the highest digital accessibility standards (e.g., WCAG).

- **Visually Impaired:** The app/portal must be 100% compatible with screen readers (like VoiceOver or TalkBack) that read out the options. The liveness check would be audio-based (e.g., "Say your date of birth").
- **Motor Disabilities:** The system must be fully navigable via keyboard, voice commands, or other assistive technologies (e.g., sip-and-puff).
- **Trusted Assistant:** As with a physical booth, the law would likely have to permit a "trusted assistant." The voter would have to check a box: *"I am using an assistant to help me cast my vote."* This *breaks* secrecy, but the alternative is *no vote at all*. This is a legal trade-off the law must explicitly make.

5. (From a Judge) How do you uphold the "secret ballot" against coercion? This is the system's greatest weakness. The primary countermeasure is the **"Last Vote Counts" protocol.**

- A voter is allowed to log in and **vote multiple times** during the polling window.
- If a person is forced to vote at 10 AM, they can secretly log in again at 8 PM and vote for their *real* choice.
- The system is designed to **only count the *last* valid ballot cast** by that voter, automatically discarding all previous ones. This makes vote-buying and coercion unreliable.

6. (From a Judge) What stops a party from capturing a village, authenticating 100 voters, and casting their votes? This is the "snatch and vote" scenario you described.

- **Liveness:** The challenge-response liveness check is the main barrier. It's difficult to spoof or force 100 people to "turn their head left" on command, one by one.

- **Time & Anomaly:** This process is *slow*—it might take 3-5 minutes per voter. AI-driven anomaly detection would flag if 100 votes are cast from the *same IP address* in a short window, potentially invalidating them pending an inquiry.
- **"Last Vote Counts":** Again, this allows those 100 voters to re-vote in private later, voiding the fraudulent votes.

7. (From a Judge) What if the ECI's database is hacked or an insider "changes" the votes? This is why **homomorphic encryption** and **threshold cryptography** are non-negotiable.

- **No Changing Votes:** Because votes are encrypted *on the user's device*, an insider cannot "change" them. They would just see a database full of gibberish.
- **No Peeking:** Because of homomorphic encryption, no one *ever* decrypts an individual vote.
- **No Rigging the Tally:** The final decryption key for the *grand total* is split into multiple "shards" held by different, high-trust authorities (e.g., Chief Election Commissioner, Chief Justice of India, a senior Opposition member). No single person *can* decrypt the result, preventing a top-level "digital coup."