# Specify The Business Problem

Whether talking about traditional paper-based voting, voting via digital voting machines, or an online voting system, several conditions need to be satisfied:

- Eligibility: Only legitimate voters should be able to take part in voting;
- Un reusability: Each voter can vote only once;
- Privacy: No one except the voter can obtain information about the voter's choice;
- Fairness: No one can obtain intermediate voting results;
- Soundness: Invalid ballots should be detected and not taken into account during tallying;
- Completeness: All valid ballots should be tallied correctly.

Below is a brief overview of the solutions for satisfying these properties in online voting systems

## Eligibility:

The solution to the issue of eligibility is rather apparent. To take part in online voting, voters need to identify themselves using a recognized identification system. The identifiers of all legitimate voters need to be added to the list of participants. But there are threats: Firstly, all modifications made to the participation list need to be checked so that no illegitimate voters can be added, and secondly, the identification system should be both trusted and secure so that a voter's account cannot be stolen or used by an intruder.

## Un reusability:

At first, glance, implementing un reusability may seem straightforward—when a voter casts their vote, all that needs to be done is to place a mark in the participation list and not allow them to vote a second time. But privacy needs to be taken into consideration; thus, providing both un reusability and voter anonymity is tricky. Moreover, it may be necessary to allow the voter to re-vote, making the task even more complex [38]. A brief overview of un reusability techniques will be provided below in conjunction with the outline on implementing privacy.

## Privacy:

Privacy in the context of online voting means that no one except the voter knows how a participant has voted. Achieving this property mainly relies on one (or more) of the following techniques: blind signatures, homomorphic encryption, and mix-networks [39]. Blind signature is a method of signing data when the signer does not know what they are signing.

## Fairness:

Fairness in terms of no one obtaining intermediate results is achieved straightforwardly: Voters encrypt their choices before sending, and those choices are decrypted at the end of the voting process. The critical thing to remember here is that if someone owns a decryption key with access to encrypted decisions, they can obtain intermediate results.

## Soundness and Completeness:

On the face of it, the completeness and soundness properties seem relatively straightforward, but realizing them can be problematic depending on the protocol. If ballots are decrypted one by one, it is easy to distinguish between valid and invalid ones, but things become more complicated when it comes to homomorphic encryption.