Trust and the machine: the nuances of electronic voting

Subhashis Banerjee *
(Views expressed are personal)

November 15, 2023

Elections should not only be fair but also appear to be fair. The incessant and disorderly public debates, suspicion, and court cases around the EVMs and VVPATs are certainly not good for democracy, and the Election Commission of India (ECI) should endeavour to put all doubts to rest. To engender complete public trust, elections need to be demonstrably and publicly verifiable.

There can be no doubt that India requires electronic voting, not only for efficiency, but also for ensuring correctness. There is no logical reason to trust the custody chain of ordinary paper ballots more, which perhaps is far easier to corrupt than the EVMs. If EVMs are not verifiable, ordinary paper ballots are even less so, and it is undeniable that public confidence in elections has only increased with the introduction of electronic voting. Nevertheless, it is also true that public trust in electronic voting is not as high as it should have been, and the ECI needs to address this urgently. However, to be able to do so, the ECI needs to be more principled and open-minded, and not resort to mere forceful proclamations that all is well. Lack of credible evidence of hacking does not imply that the process is unhackable, and it is specious to argue that nothing is wrong because complains supposedly arise only when there are unfavourable outcomes.

Consider first an EVM without VVPAT, where votes are recorded electronically by press of a button, and the voter cannot examine what has been recorded. Without establishing the integrity of the EVM beyond all doubt, there is no way to provide a guarantee to a voter that the vote is cast as intended (recorded correctly in the EVM), recorded as cast (what is recorded in the EVM is what is collected in the final tally) and counted as recorded. It is well known that establishing the correctness of a system as complicated as an EVM is an intractable problem. There is actually a theorem to that effect. It is also well known that testing is never adequate to establish the correctness of an EVM, and tests can detect only a small fraction of possible software or hardware errors. Also, verifying the signature of the source code or embedded software does not guarantee the integrity of an EVM.

If the correctness of an EVM cannot be established, then it is impossible to predict whether an EVM can be hacked or not, or determine whether all EVMs used in an election are identical in functionality. Also, that an EVM has not yet been hacked provides no guarantee whatsoever that it cannot be hacked. And, the onus of proving correctness is on the ECI, and not on hackers to demonstrate incorrectness; that is not how computer security is argued. Thus, elections must be conducted assuming that the electronic voting machines may possibly be tampered with. The only way to do so is to make the voting protocol software independent, as argued by Ron Rivest from MIT in 2008 in a famous paper published in the Philosophical Transactions of the Royal Society. This is not to say that software cannot be used, but that an undetected change is software or hardware should not cause an undetectable change in the election outcome.

*Professor of Computer Science, Ashoka University. Also associated with the Centre for Digitalisation, AI and Society at Ashoka University. Email: suban@ashoka.edu.in

Hence, the various civil society demands that source code should be made public, or that EVMs should be standalone and use only one-time programmable chips etc., only serve to detract from the main issue. Even if all these demands are met (and they should be) an EVM will still not be software independent and hence not verifiable.

Conventional wisdom in electronic voting demands that any reasonable threat model – for both correctness and vote secrecy – must assume that an adversary may control the voting hardware, one or more insiders or polling officials, and even voters. An election process is acceptable only if it is robust with respect to such a threat model. Indeed, there are several electronic voting protocols that measure up to such standards, but all of them use cryptographic commitments. They thus fail the test stipulated by the German Constitutional Court in 2009 that an election process is valid only if all its essential steps can be ascertained by the common man, without requiring any special knowledge or certification from experts. EVMs also fail the test.

A standard way to make an electronic voting process software independent, at least approximately, is to use VVPATs, provided of course they are counted. Such dual-voting protocols have three essential requirements – the VVPATs should be truly voter-verified, the electronic and the VVPAT tallies should be cross-checked against each other, and there needs to be a definite rule to break the tie if the cross-check fails.

The ECI's current VVPAT system is not truly voter-verified because it does not provide the necessary agency to a voter, and there is no principled method for dispute resolution. The correct VVPAT protocol would be to allow a voter to approve the VVPAT slip before the vote is finally cast, and to provide an option to cancel her vote if a discrepancy is noticed. It is now well understood that the only way to do so, without trusting machines and buttons, is to allow the voter to obtain the VVPAT slip and cast it in a box with her own hand. There are standard ways to mitigate the fear that a voter may cast a bogus slip and try to discredit the election.

Finally, there are standard and well-established methods called Risk-Limiting Audit (RLA) for cross-checking the electronic tally with VVPAT counts. The current stipulation of auditing five EVMs per assembly constituency is without any statistical basis. RLA verifies, with high confidence, that the declared outcome matches the one that would have been determined with a full manual count of the VVPATs. RLA is also efficient, and usually requires far less than full count unless the margins are really small. If required, independent systems of mechanised sorting and counting may also be set up to facilitate RLA. In any case, efficiency cannot possibly be privileged over correctness.

The above are also the recommendations of the Citizens' Commission on Elections headed by Justice Madan Lokur of which I was a member.