Barking up the wrong tree

Subhashis Banerjee *

January 8, 2023

In a welcome move the Election Commission of India (EC) has announced its intention of introducing remote voting across the country, a facility to enable voters who are residents elsewhere to vote in their home constituencies. Considering that India has a significant fraction of migrant population, this provision is much required. The EC proposes using isolated remote voting machines (RVM), which are multi-constituency extensions of the extant EVMs, to enable voting from remote locations. EC has also announced that they will demonstrate the prototype RVMs to representatives of all political parties on January 16.

However, EC's overemphasis on the RVM appears to be misplaced. There is much more to remote voting than voting electronics, and EC's proposal appears to be sketchy and grossly inadequate. Several crucial questions arise.

First, how will it be ensured that all those who wish to apply for remote voting are able to do so without let or hindrance, and that all applications are processed fairly without inadvertent or selective exclusions? Under what conditions will remote voting be denied? It is not sufficient to just define a protocol, but it needs to be ensured that all applications – and the decisions on them – are publicly verifiable, from both remote and home locations. This can only be done with verifiable zero-trust technology that is crucially linked to digitisation of electoral rolls, which, by itself, requires a threadbare examination.

Second, how will it be ensured that a person allowed to vote remotely is invalidated for local voting and also that nobody is incorrectly invalidated? Since the two lists will be at different locations, the correctness will not be easy to demonstrate in a publicly verifiable way. For example, even if the lists are shared over the internet, how does one guarantee that indeed it is the shared lists that are used?

Third, how will the votes – both the electronic votes and the VVPAT slips – be consolidated and counted? Will the counting and VVPAT audit happen at the remote location, or at the home constituency after consolidation? If it is the latter, then how will it be ensured, verifiably, that the consolidation has happened correctly? If it is the former, then disclosing the remote voting results for a small number of remote voters of a constituency at any one location will compromise vote secrecy.

Fourth, who will be the polling agents at the remote locations? How will it be ensured that in a different political environment at the remote site a remote voter will not be coerced?

The above problems are not insurmountable, but they will require considerably more due diligence. They will also require a significant shift of emphasis from designing electronics to ensuring verifiability. After all, the effectiveness of a remote voting procedure cannot be ascertained merely from a demonstration of a voting hardware. Neither is the design of a voting protocol an electronic system design problem.

*Computer Science, Ashoka University, Plot #2, Rajiv Gandhi Education City, P. O. Rai, Sonepat, Haryana 131029 (on leave from IIT Delhi). Email: suban@ashoka.edu.in

Unfortunately, this misplaced emphasis on unverifiable voting machines has been a long-standing, ostrich-like problem with the EC. That the correctness of a machine with the essential properties of an EVM is unverifiable is a well-known theoretical result at least since 1992 – notwithstanding the indignant protestations by election commissioners to the contrary – when VVPAT was first proposed by Rebecca Mercuri. Since then, the conventional wisdom in electronic voting – which is not to be conflated with an EVM – has evolved towards the principles of *verifiability* and *software-independence*.

This is not to say that software cannot be used in electronic voting, but that an undetected change or error in the software should not cause an undetectable change or error in an election outcome. It is well known that a stand-alone EVM, whichever way its components are internally connected, cannot be software-independent which is a necessary condition for verifiability.

It is this understanding – and the requirement of public verifiability of elections – that led the German Constitutional Court to pronounce against EVM use in 2009, an exhortation that is honoured not only in Germany but also in many other jurisdictions across Europe and America as well, and Pakistan. It has also led the US National Academy of Sciences to recommend against purely electronic voting in a public report in 2018. One way out – as an approximation to software-independence – is to audit the electronic results with a count of the VVPATs, either with a complete count or that of a statistically significant sample. The procedure for doing this, called Risk Limiting Audit, is well established in voting literature. Unfortunately, it appears that election results are declared in India without any VVPAT audits at all. Even the Supreme Court's stipulation of auditing five randomly selected EVMs per assembly constituency against VVPAT counts appears to be without any sound statistical basis. The EC has also ignored the plea of a 2020 report of a Citizens' Commission on Elections, of which I was a part, on verifiability and VVPAT counting.

While usability demonstrations are essential for public acceptability, they do not assure safety or security. Modern computer and digital security is not established by demonstrations or forceful proclamations, but by articulating rigorous threat models and proving verifiable robustness against them. Cryptography may help in doing so. After all, one cannot bring digitisation to public life but leave the rigours of computer science behind.